Study & Analysis of Copy-Move Forgery Detection in Digital Image using MATLAB

Thesis

Submitted to the

G.B. Pant University of Agriculture & Technology,

Pantnagar-263 145, Uttarakhand, India

By

Rachana

B. Tech. (Computer Science & Engineering)

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

Master of Technology

(INFORMATION TECHNOLOGY)

July, 2016

ACKNOWLEDGEMENT

I am overwhelmed with joy to evince my profound sense of reverence and gratitude to Mr. Ashok Kumar, Assistant Professor, Information Technology Department, College of Technology and chairman of my Advisory Committee, for his insightful, critical criticism and invaluable guidance during the course of present investigation.

I am immensely indebted and owe my due regard to Dr. H. L. Mandoria, Professor & Head, Information Technology Department, Binay Kumar Pandey, Assistant Professor, Information Technology Department, and Rajesh Shyam Singh, Assistant Professor, Information Technology Department the members of my Advisory Committee for their persistent encouragement and support. I wish to express my thanks to Dr. H. C. Sharma, Dean, College of Technology & Dr. N. S. Murty, Dean, Post Graduate Studies. I have immense pleasure to thank all the teachers and staff members of the Information Technology Department.

I would like to express my sincere thanks to my batch mates Sonal paliwal, Ujwal Singh Vohra, Anamika, Akansha Pandey, Bhoomika pandey, Piyush Kothyari, Navneet Kashyap and Ravish Dubey.

A debt of gratitude is owed to the Information Technology Department, Mr. Ratnesh Shrivastava, Mr. Sanjay Joshi, Mr. Subhod Prasad, Mr. Govind Verma and Ms. Shikha Goswami for getting all sorts of help from them during my research work.

I feel extremely proud to express my profound regards, stupendous gratitude beyond accountability to my beloved Mother, Mrs. Santosh for her constant love and moral support. Blessings of my Father, Mr. Jagdish Prasad, as every problem associated were overcome due to their blessings.

The financial assistance provided by TEQIP-II, Non-GATE Fellowship is gratefully acknowledged.

Last but not least ,I record my sincere thanks from the core of my heart to all the well-wishers whose blessings propelled me to achieve my dreams and I ever remain thankful to all those who could not find separate names but had directly or indirectly helped me.

Rachana

(Rachana)
Authoress

Pantnagar
July, 2016

CERTIFICATE-I

This is to certify that the thesis entitled **"Study & Analysis of Copy-Move Forgery Detection in Digital Image using MATLAB"** submitted in partial fulfillment of the requirements for the degree of **Master of Technology** with major in **Information Technology** of the College of Post graduate Studies, G. B. Pant University of Agriculture & Technology, Pantnagar, is a record of *bona fide* research carried out by **Ms. Rachana, Id. No. 48177** under my supervision and no part of thesis has been submitted for any other degree or diploma.

The assistance and help received during the course of this investigation have been acknowledged.

(Ashok Kumar)
Chairman Advisory Committee

Pantnagar
July, 2016

CERTIFICATE-II

We, the undersigned, members of the Advisory Committee of **Rachana**, **Id. No. 48177**, a candidate for the degree of **Master of Technology** with major in **Information Technology** agrees that the thesis entitled **"Study & Analysis of Copy-Move Forgery Detection in Digital Image using MATLAB"** may be submitted in partial fulfillment of the requirements for the degree.

(Ashok Kumar)

Chairman Advisory Committee

Rajesh S. Singh

(Member)

Binay kumar Pandey

(Member)

TABLE OF CONTENTS

S. No.	CHAPTER	Page No.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

JPEG:	Joint Photographic Experts Group
SNR:	Signal to Noise Ratio
DWT:	Discrete Wavelet Transform
SVD:	Singular Value Decomposition
FMT:	Fourier-Mellin Transform
PCA:	Principal Component Analysis
DCT:	Discrete Cosine Transform
SIFT:	Scale Invariant Feature Transform
MLBP:	Multi-resolution Local Binary Patterns
RANSAC:	RANdom SAmple Consensus
TP:	True Positives
FP:	False Positives
TN:	True Negatives
FN:	False Negatives
GNU:	recursive acronym for GNU's Not Unix
GIMP:	GNU Image Manipulation Progr

Chapter 1 INTRODUCTION

1.1 Image Forgery

In current era, in which we are living, digital images have significant importance because they have become a main source of information circulation. Information expressed in thousands of words can be simply expressed in a simple image. The advancement in digital photography in the recent decades increased the use of pictorial information and makes it easier.

In today's modern life, in which we are living, Digital images play very important role in various fields. They are extensively used in different applications in the field of military, news, medical diagnosis and media, to mention a few. In today's digital age, for example, cameras, software, and computers and the wide spread via the internet, digital image can be taken as a vital source of information. But to believe what we see, we must make sure that the image is original. Thus the images are required to pass the test its reality, integrity and authenticity.

Due to the expansion in technology of digital image, and availability of low-cost hardware and software editing tools, Digital images are susceptible in the sense that, it can be effortlessly manipulate to hide or alter the meaning. It has become difficult to trace these modifications; sometimes it is challenging to know whether the image is tampered or not by the naked eyes. The purpose of such manipulation in many cases is to deliberately affect the awareness of the recipient. So, we need techniques to help validating the authenticity of the image and integrity from tampering and alteration **Minakshi *et al.* (2003).**

Due to the arrival of high resolution digital cameras and image processing tools, different forensics-related questions arise such as, how an image was acquired? Was it captured using digital devices (cameras and scanners) or artificially generated using computer software? Is it authentic or it has undergone any kind of manipulation after capturing? The answers to such forensics questions are related to find the origin of the digital image to its creation process. The field of digital images forensics has emerged and developed over the past few years as a solution to these growing challenges. The forensic analysis for digital images provides helpful information to law enforcement, security, and intelligence agencies **Sunil *et al.* (2011)**.

1.2 Motivation

We see and use the images in our daily lives at very large scale; also we are exposed to it in many places and different ways, such as internet, advertising media, TV and newspapers. But, in today's digital age, it has become not difficult to change the information depicted by an image without any noticeable traces. But the truth is that with the easiness of digital image manipulation provided by the growth of computer technology, we have to be aware about what we are seeing. There are more and more sophisticated and widespread digital techniques have the ability to tamper the digital image. The purpose of tampering of digital image is to deliberately affect the awareness of the recipient. The following examples illustrate some of the forged images.

(a) Original Image **(b) Tampered Image**

Fig. 1.1 Example for tampering of digital image

Fig. 1.1 shows one example of copy-move forgery. In the figure, shows the original image part (a) two pen, while in part (b) shows the tampered image with a single pen to create forgery in the image.

The proficiency of doctored image is shown by the above example. Moreover, many post processing operations can be used in the tampered region such as noise addition, JPEG compression, blurring, etc. in order to conceal the tampering clues. With all these tampering techniques, it becomes impossible to detect image tampering by the naked eyes. Generally, it means that the trustworthiness of digital images is questioned and their content integrity can no longer be completely trustworthy. We believe that, recovering the community confidence toward digital image contents is very important.

1.3 Aim

The main objectives of the research work are as follows:

- Improve the time complexity of copy move forgery detection in digital image.
- Formation and development of a database for image forgery detection.

Now these days, Digital image forgery becomes a common information falsification trend. This is generally done due to the largely available contemporary editing software and superior digital cameras. In today's digital age, it is feasible to add or remove important features from an image without any clear traces of alteration. So there is an imperative issue to identify the authenticity of digital images in various fields such as forensics, criminal investigation, surveillance system, intelligent system, medical imaging and Journalism. Digital Image forensics finds the authenticity of the images. Digital Image Forensic is rising and swiftly growing field of image processing area to find the authenticity of digital image.

1.4 The Need for Detection of Digital image Forgeries

Digital image forgery means the purposely manipulation of digital image, for the purpose of altering the semantic meaning of the visual message included in that image. . With the enrichment of technology and ubiquitous availability of image processing tools, Due to the widespread techniques for tampering, every digital image are taken as vulnerable, due to the sophisticated techniques for tampering.

In the current era, digital images play important role in various field, in daily life applications in the area of military, news, medical diagnosis and media. So, truthfulness of digital image is important aspect in daily life applications. Tampering in digital image is not new; digital image forgery is very easy due to largely available tampering techniques and tools **Sevinc *et al.* (2008).**

Digital images play important role in daily life applications in the area of military, news, medical diagnosis and media. Due to the widespread popularity of digital images and powerful image processing tools, it is crucial to verify the integrity and authenticity of the digital images recognize their sources, and detection of forgeries **Judith et al. (2010).**

Digital image is prone to change. The availability of powerful, user friendly

computer graphics editing software to end users makes the job of manipulating image easier than ever. With the fundamental knowledge of digital image and the tools in a computer graphics editing software will be able to change an image with ease.

Now, the digital revolution and matter concerned with multimedia security have also various approaches to detecting digital image tampering. Forged image can be used to misrepresent something, to boost a negative or positive image of someone, and etc. Therefore each and every digital image must therefore be subject to test for authenticity in many areas-forensic investigation, criminal investigation, surveillance system, intelligent system, medical imaging and journalism. Digital image forgery detection techniques are attempted to check the integrity and authenticity of images. These detection approaches fall into two categories: (1) active and (2) passive (blind) approaches. The active methods fall into two categories: (1) The data hiding approach (e.g. watermarks) and (2) the digital signature approach. I emphasized on blind methods. These methods work in the absence of any protecting approach and without using any previous information related to the image.

In earlier days, when digital watermarks or signatures were not available, blind approach was the only way to verify the integrity and authenticity of the digital images. Image forensics is a fast growing research field to check authenticity and integrity of digital images.

1.5 Type of Digital Image Forgery

There are different types of digital image forgery. All of these fall into three major groups, based on the process comprised to create the fake image. The groups are image retouching, image splicing, and image copy move forgery. Fig. 1.2 shows block diagram of different type of forgeries in digital images.

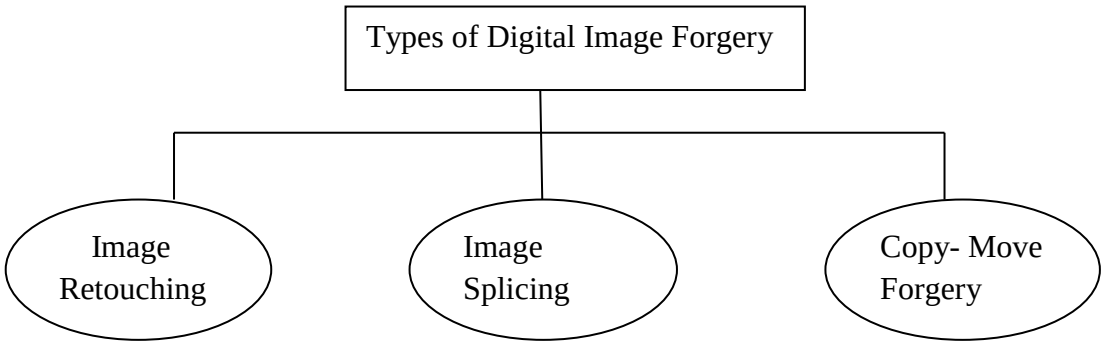


Fig. 1.2 Important and common types of digital image forger

1.5.1 Image Retouching

Digital images retouching is known from the early years of photography. Since then, it was used by portrait photographer to improve their sales. Digital images retouching is considered to be the less harmful kind of digital image forgery, since it does not make seriously changes to the visual message of an image. Alternatively it can be used to enhance or reduce digital images features as in Figure 1.3. We can see the image retouching, and the difference between left image and right images (enhanced) clearly.

Fig. 1.3 Example of Image Retouching

1.5.2 Image Splicing

In image splicing, fragments from two or more images are combined to create a new image. Fig. 1.4 shows a sample of image splicing. Image splicing technique may change the semantic meaning of digital images more aggressively than image retouching.

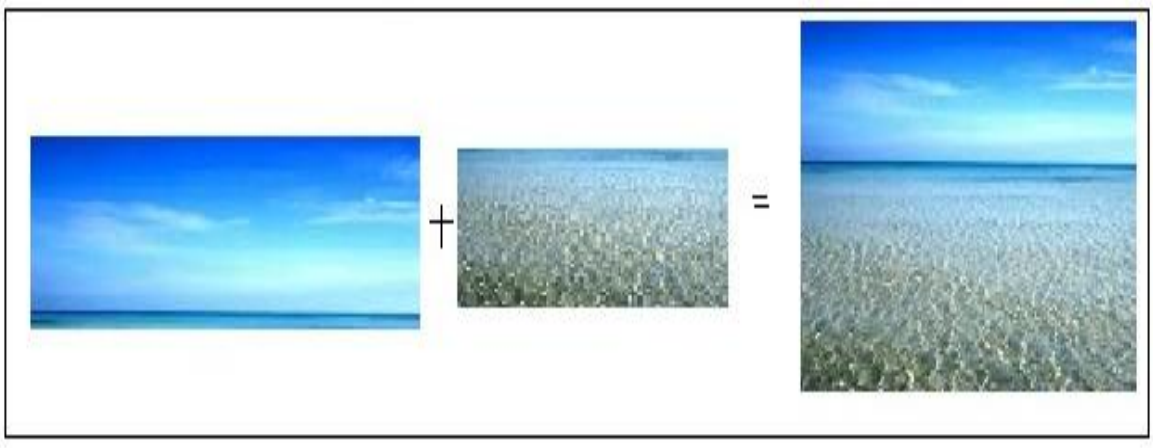


Fig. 1.4 Example of Image Splicing

1.5.3 Copy-Move Forgery

Copy-Move forgery of digital images can be considered as a special case of image splicing, where the tampering occurs within a single image and no need for multiple

images. In simple words we can say that a part of the image is copied and then pasted in a desired location within the same image. Some post processing such as blurring, median filtering, is usually applied region to decrease the effect of irregularity between the original and pasted region.

We can see from Figure 1.5, the original image containing only two balloon while the forged image containing three balloons. Here in forged image blue balloon is copied and pasted to just right to the blue balloon.

(a) Original Image (b) Forged Image

Fig. 1.5 An example of Copy-move Forgery

1.5.4 Type of copy-move forgery

There are also many types of copy-move such as just a copy-move (Figure 1.6 shows an example), copy-move with rotation (Figure 1.9 shows an example), copy move with a different scale (Figure 1.8 shows an example) and copy-move with reflection (Figure 1.7 shows an example).

Fig.1.6 Example for just Copy-move

Fig. 1.7 Example for Copy-move with reflection

Fig. 1.8 Example for Copy-move with different scaling

Fig. 1.9 Example for Copy-move with rotation

1.6 Types of Image Authentication

The concerns of multimedia security have led to the progress of several approaches to detect the tampering in digital image. Commonly, the two types of approaches that can be utilize for image tampering detection, active authentication and passive authentication, as shown in Figure 1.10.

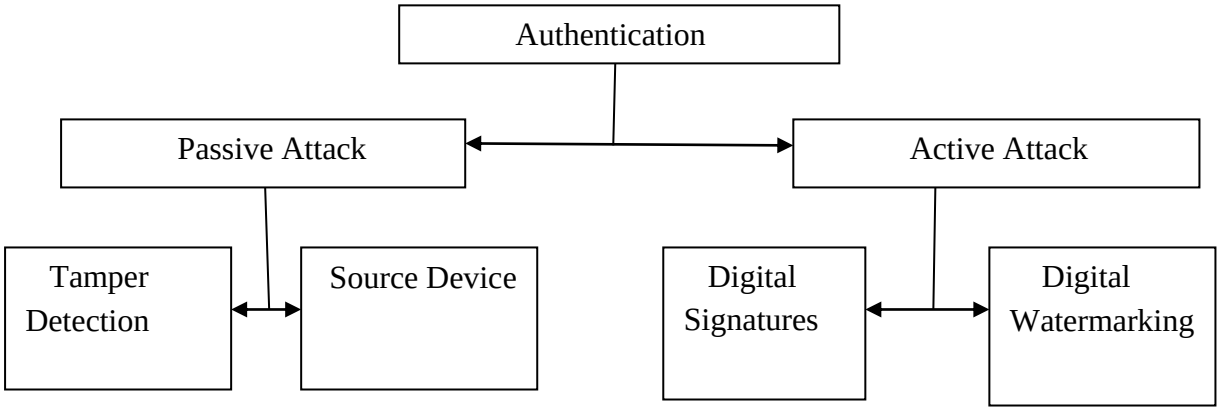


Fig. 1.10 Types of image authentication

1.6.1 Active Authentication

Digital watermarking: In this passive approach hides a watermark into the image at the capturing end and extracts it at the authentication end to analyze whether the image has been tampered or not. In digital watermarking a specific digest is attached inside an image at the capturing end. After that digest can be extracted from the image later time to prove

authenticity. If the extracted digest is different than the original that was attached inside the image at the image acquisition, it shows that the image was altered after the recording time.

Digital signatures: In digital signature technique, the unique features of a digital image are extracted at the capturing. During authentication, same technique is used to generate the signature again. The authenticity of the image may be identified through comparison.

1.6.2 Passive Authentication

This is the process of authenticating digital images without using any auxiliary information apart from the pictures themselves. Now, the Passive approaches are further grouped into two categories: the source device identification and tamper detection.

Source device identification: This category works on the traces. For instance, the truthfulness of digital image is important aspect in courtrooms, where as they are used by evidence, the identification of image acquisitioning device (source) would be of interest for image authentication. For this source device (camera) identification method (Exchangeable Image File) is being used determining the image authenticity. There are different models of cameras or even different exemplars of the same camera models. We use the camera fingerprint to differentiate these different models of cameras or even different exemplars of the same camera model.

Tamper detection: Tampering a digital image without any obvious trace. Due to the widespread digital tampering techniques is not tough to alter the meaning of the digital image. In general, modification in color and contrast is not taken as malicious forgery. So adding, removing or re-touching an object in the digital image which would make the tampering hard to detect is taken as malicious forgery. In the next section we will review the most important and common types of this category.

1.7 Thesis Outline

This thesis is organized into five chapters. The rest of the thesis is organized as follows: The present chapter is followed by chapter 2, which provides a review of the previous work done in the field of copy –Move forgery detection. It begins with the basic terminology used in image forgery and then gives a brief review of the previously

developed techniques according to the different types of forgery. It provides the review information in a chronological order.

Chapter 3 describes the proposed method. This chapter is divided into two sections, in the first section a common workflow graph of digital image forgery detection is exercised and in the later section the step by step representation of the proposed method is given.

Chapter 4 discusses the experimental results with the proposed method and the comparison of obtained results with the previous algorithm proposed by **Sunil *et al.* (2013).**

Chapter 5 presents the research conclusions and the suggestions for further studie

Chapter 2 REVIEW OF LITERATURE

2.1 Literature Review

A literature review helps to locate and summarize the study of a specific topic. For mixed methods study, literature review is defined as a consistent way for major type of study either quantitative or qualitative. Reliable sources such as IEEE and books on Digital Image Forgery were used for detailed literature review in order to acquire relevant information, which assisted in answering the research questions.

Now a day, many image tampering techniques are available which are frequently used to alter the information represented by an image. Copy-Move attack is very common type of tampering technique, where a part of an image is copied and pasted elsewhere in the same image to conceal a special object in the original image. Duplicate parts keep the identical properties since they come from the same image.

Fridrich *et al.* (2003) primarily presented a technique to espy duplicated region in forged image. In this paper a discrete cosine transform (DCT) based block matching approach is used to detect copy-move forgery. The author uses block tiling approach to detect duplicated region. So, that whole image is divided into a fixed size overlapping blocks and then DCT coefficient corresponding each block is calculated and thus formed a DCT feature matrix. Then these blocks are arranged in Lexicographical order. Thus these considered neighbor region are compared in the matching step .This technique in some complicated manipulation techniques like blurring or random noise addition it is not easy task to detect the forgery.

To make the computation faster, **Popescu *et al.* (2004)** proposed a method based on Principal Component analysis (PCA).Due to the characteristics of PCA the number of features required to present a block were reduced as the half of the numbers of the features used by **Fridrich.** So this method has better time complexity and has better immunity to random noise and JPEG compression. But the method has one disadvantage that not robust against small rotations of copy-moved regions.

A method based on Intensities to detect Copy Move Forgery is proposed by **Luo, Huang and Qiu (2006).** They proposed a robust method can detect duplicated

region if the tampered image were undergone some attacks (like lossy compression, noise contamination, blurring and combination of these). This is also a block matching algorithm. In this method seven characteristics features Cj (j=1,2,….,7) are computed for each overlapping block of an image of size M*N. In which C1, C2, C3 are average red, green and blue components respectively. Then each block is divided into two equal parts in four directions and corresponding features are computed in each direction as C4, C5, C6 and C7 respectively. After that the copied regions are identified based on some preset threshold values. And claim a better computational complexity.

A method was based on blur moment invariants proposed by **Mahadian and Saic (2007)**. This method can detect the duplicated region even if the doctored images were undergone post processing such as blurring, added noise or arbitrary contrast changes. The author first divides the whole image into a fixed size overlapping blocks and each block is represented by blur invariants. The dimension of the blocks representation is reduced by using the principal component transformation and improve Popescu's algorithm by adopting blur moment invariants.

There is a technique to espy copy-move forgery, which is based on filtering operation and nearest neighbor search proposed by **Dybala *et al.* (2007).** Firstly, in this technique the filters (like laplacian) are used to smoothen the pasted region. Then a Kd-tree method is used for clustering of the most similar blocks. Root mean square error is used as matching criterion. The method shows a reasonable robustness to high quality image compression.

Li *et al.* (2007) proposed a technique to espy copy-move forgery based on Discrete Wavelet transform (DWT) and Singular Value Decomposition (SVD). Firstly, the author applied the DWT is applied to the image, and SVD is used on fixed-size blocks of low-frequency component in wavelet sub-band to yield a reduced dimension representation. Lexicographically sorting is used to sort the SV vectors. So that similar image block will be close after sorting. And finally these blocks compared during detection steps. This method works well even if the image is highly compressed or edge processed.

Myna *et al.* (2007) proposed a method based on log-polar coordinate and Discrete Wavelet Transform (DWT). For the dimension reduction DWT is applied on the input image. And then sub blocks of the images are mapped on the log-polar coordinate to acquire a matrix corresponding to each block. Lexicography sorting is used to bring similar rows closer. Phase correlation was employed for similarity criterion. This method has lower time complexity. This method is robust against geometric operation (scaling and rotation).

Zhang *et al.* (2008) a new approach is suggested to espy duplicated region in the doctored image. In this method applied DWT on the image to reduce the size of the image .Only low-frequency sub has been taken and then further divided low-frequency band into four non-overlapping sub-images and phase correlation is adopted to compute the spatial offset between the copy-move regions. Then, pixel matching is applied for detecting the forged region. This method is robust in the highly compressed image and also has lower computational time compared with other method.

A novel approach is introduced by **Huang *et al.* (2008)** based on Scale Invariant Feature Transform (SIFT). In this approach SIFT descriptors of an image are extracted. As SIFT descriptors were invariant, this scheme were robust against changes in illumination, rotation, scaling etc. This key feature of SIFT descriptors is explore to detect the copy-move forgery. So SIFT features of copied and pasted region are matched to detect the tampering. This method performs very well up to JPEG compression 40 and SNR 20db. But problem of false positive is detected for very small block size.

There is a technique based on Singular Value Decomposition proposed by **X. Kang *et al.* (2008)** The author first divides the whole image into a fixed size overlapping blocks and SVD is applied on these blocks..Then lexicographically sorting is performed for similarity matching & thus forged region is detected in the tampered image.

In order to espy copy-move forgery in the forged images through rotation and scaling, blurring, noise addition and JPEG compression, image forgery detection based on Fourier-Mellin Transformation (FMT) is proposed by **Bayram *et al.* (2009)**. Lexicographic sorting is used to neighboring the similar block and Counter bloom filter

are used in spite of lexicography sorting to compare the similar blocks.

There is a technique based on Singular Value Decomposition (SVD) is suggested by **Ting and Rang-ding (2009).** In this method, Author first divided the images into several small overlapping blocks, then SVD is applied to every block and thus unique singular values feature vector is extracted for each block. After this extraction, matching is done by transforming each block feature into k-d tree. A threshold value is used to increase the robustness.

Wang, Liu, Li, Dai and Wang (2009) proposed a method, Firstly Gaussian pyramid is used for the dimension reduction of the image. And the Hu moment is applied to the fixed sized overlapping blocks of low-frequency image. After that sorting of eigenvector is done using Lexicographic sorting. After that similar eigenvectors matched by a certain threshold value. And a mathematical morphology operation is applied to locate the tampered part.

There is a new approach based on intensities is presented by **Lin *et al.* (2009).** First the image is divided into several overlapping blocks, further divided into four blocks, after this calculated the average intensity of a single block by using the intensity of the four sub-blocks. Relative intensity is calculated. To obtained feature vectors, relative intensity is calculated for all the blocks. These feature vectors are integers; hence they used radix sort method instead of lexicographical sorting. Shift vector is used to determine tampered region and forgery detection. This method is efficient against JPEG compression and Gaussian noise.

Wang, Liu, Li, Dai and Wang (2009) . They proposed a method which uses Gaussians pyramid method to reduce the dimension of the image .In this method circle block is used, then calculated feature. Lexicographic sorting is used to sort the feature vector and find the matching feature vector by adjusting threshold value.

A technique based on DWT (Discrete Wavelet Transform) is suggested by **S. Khan and A. Kulkarni (2010).** In this proposed technique DWT is applied to the suspected image to yield a reduced dimension representation. Then this reduced dimension image is divided into overlapping blocks. After that lexicographic sorting is applied on each block and similar blocks are matched using Phase Correlation. Due to

DWT usage this approach drastically reduces the time needed for the detection process and increases accuracy of detection process.

S.-jin Ryu and M.-jeong Lee (**2010).** Zernike moments based detection approaches the flat copied region is detected and also invariant to different operations like JPEG compression, rotation, blurring and AWGN. The algorithm exhibited robustness against different degrees of rotation and high detection rate but not for the scaling.

There is a technique based on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) in order to robust against translation-flip and translation-rotation of duplicate region is presented by **Bashar *et al.* (2010).** In this method, Author first divided the images into several small overlapping blocks .Each block is transformed by DWT or KPCA. DWT is applied on the image to reduce the size and obtained the low approximation coefficients. KPCA is used for feature collection. Whole image is then represented by a matrix, where each row vector corresponds to a block and lexicographic sorting is then applied to matrix.

A method is suggested to detect tampering (copy move forgery) in digital image by **Kang *et al*. (2010).** In this method divided the image into sub-blocks and used improved SVD. Then, similarity matching is performed on the lexicographically sorted SV vectors and the forged region in the images is detected.

There is a technique based on Discrete Wavelet Transform (DWT) and Principal Component Analysis-Eigenvalue Decomposition (PCA-EVD) is presented by **M. Zimba and S. Xingming (2011).** DWT is applied on the image to reduce the size and obtained the low approximation coefficients. Here Principal component analysis is used for reduced dimension representation .This technique accurately detects copy move forgery if the forged image were not undergone some specific image manipulations as long as the copied region is not rotated or scaled.

There is a technique based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) is presented by **M.Ghorbani *et al.* (2011).** DWT is used for dimension reduction and image divided into subbands and then performs DCT-QCD

(quantization coefficient decomposition) in row vectors to reduce vector length. After that lexicographically sorting .Finally, the shift vector is compared with threshold.

Muhammad *et al.* (2011) proposed a technique based on Dyadic Wavelet Transform (DyWT). Due to the characteristics of DyWT (shift invariant) is used. So, it is more applicable than discrete wavelet transform (DWT) for data analysis. In this technique, decomposes the input image into approximation (LL1) and detail (HH1) subbands. Further those subbands(LL1 and HH1) are divided into overlapping blocks and after that measure the similarity between blocks. A method based on Dyadic Wavelet Transform (DyWT) in which both the LL and HH sub bands are used to find the similarity between the blocks of image.

Later on, another technique based on undecimated wavelets and Zernike moments to detect copy move forgery is presented by same author **Muhammad *et al.* (2011**). UWT is translation invariant, while ZM is scale and rotation invariant. In this technique, UWT is applied to find its approximation and ZMs are extracted from the approximation. By using the Euclidean distance compared the similarity of the moments between the blocks of an image. This algorithm is robust against different degree of rotation and high detection rate but for the scaling.

There is an Improved DCT-based technique is suggested by **Yanping Huang *et al.* (2011)** to detect copy move forgery robust against JPEG compression, blurring or additive white Gaussian noise. Firstly, Discrete Cosine Transformation (DCT) is applied on fixed-size overlapping blocks of input image.DCT coefficient are obtained from each block to represent its features. To reduce the dimension of the features, Truncation is performed. Lexicography sorting is performed on calculated feature vectors. Duplicated region blocks are compared in the matching step.

There is a technique robust against some post processing operation such as reflection, rotation and scaling is proposed by **Bravo-Solorio and Nandi (2011)** .They divided the image into block of pixel by sliding pixel by pixel of a particular size in a raster scan order. Then they obtained color dependent feature vector, they did this to reduce the dimension to reduce the number of searches and thus increases the efficiency. The calculation of four features out of which three features are independently computed as red, green and blue components. The fourth feature is calculated as the entropy of

luminance channel. They used this fourth feature to discard blocks with insufficient textural information. Then lexicographically and matching is performed. And filtering is also done in this method because it produces lot of matches.

A technique is presented by **S. D. Lin et *al.*(2011)** to espy the image splicing and copy move forgery in the forged image. Firstly, the image is divided into blocks YCbCr color space. The image is divided into sub-blocks and DCT is used for feature extraction for image splicing. SURF is used for copy move forgery detection.

Sridevi, Mala and Sandeep (2012) proposed a method for detection of copy move forgery in parallel environment. The methods begin with dividing the image into several blocks. Feature extraction is done for every block using intensity. The last two locations of the feature vectors store the block position. They developed one more algorithm for parallel sorting. Lexicographical sorting is done using radix sort method in a parallel way. They found the duplicated regions by matching of features and these blocks are mapped on to the image using the location stored in the vector. This method shows improvement in performance over other conventional techniques.

Nguyen and Katzenbeisser (2012) proposed a method which is based on radon transformation and phase correlation. In this method, Feature extraction is done by using Radon transform and phase correlation is used to match duplicated blocks. This proposed method is robust against rotation with angles smaller than 4◦ and Gaussian noise addition with SNR values larger than 35 db.

A technique based on method PHT (Polar Harmonic Transform) is presented **by Li, Li and Wang (2012**). Feature extraction is calculated by using PHT and they accomplished matching using PHT features. This technique is able to find a copy-move forgery which involves block rotations and geometric transformations.

There is a technique most robust to multiple copy move forgeries, noise and blurring, but not robust against compression, rotation and scaling is suggested by **Y. Cao, T. Gao, L. Fan, and Q. Yang (2012)** .In this method**,** author first divides the whole image into a fixed size overlapping blocks and discrete cosine transform (DCT) is applied to each block, thus, the DCT coefficients is obtained. Secondly, each cosine transformed block is represented by a circle block and four features are extracted to

reduce the dimension of each block. After that lexicographic sorting is used to sort the feature vector and then duplicated image blocks will be matched by a preset threshold value. The technique not only reduced the feature length but showed robustness against detection of multiple copy move forgeries, noise and blurring, but not robust against compression, rotation and scaling.

There is a technique based on Polar Harmonic Transform (PHT) proposed by **Leida Li *et al.* (2012).** In order to find the duplicated region i.e. copy-move forgery when the copied region is rotated before being pasted. The method was based on Polar Harmonic Transform (PHT) is to extract the features of the circular blocks, which are then used to perform block matching.

A method based on Weber law descriptors (WLD) proposed by **Muhammad Hussain, Ghulam Muhammad (2012)**. WLD is a robust local descriptor. In this method, input RGB image is converted into chrominance component. And then the chroma component (either Cb or Cr) is used to extract image features. Multi-resolution WLD extracts the features from chrominance components, which can give more information that the human eyes cannot notice. A support vector machine is used for classification purpose. This method gives accuracy rate up to 91 % with multi-resolution WLD descriptor on the chrominance space of the images.

There is a technique in order to achieve the robustness against additive noise and blurring is suggested by **Bo Xu, Guangjie Liu and Yuewei Dai (2012).** A non block-matching based method is proposed exploiting phase correlation, which is a fast method to detect cross covariance.

A novel method using transform invariant features with respect to scaling, rotation, blurring, compression and additive noise is proposed by **P. Kakar and N.Sudha (2012).** In this method MPEG-7 image signature tool is used for copy move forgery detection and this method also reduces the false positives by using the procedure of multi-hypothesis matching.

There is a technique based on local binary pattern (LBP) and neighborhood clustering is proposed by **Motasem AlSawadi *et al.* (2013) .**Method utilizes three color component and Then LBP histograms are calculated from each blocks component. LBP

is used to find texture patterns. The neighborhood clustering technique is also introduced to reduce the false positives.

Jie Hu *et al.* (2013) proposed a method was based on DCT .First the image is divided into 8*8 block then applied DCT on each block. DCT coefficients were grouped to reduce the dimension according to the frequency property. Finally, the distance of eigenvectors, instead of the DCT coefficients, was taken as the eigenvalue to fulfill the block matching. Method is robust to blurring and noising.

There is a technique based on SIFT in order to achieve robustness against complex geometrical transformation such as rotation and scaling in large degree and illumination changes suggested by **Bo Liu and Chi-Man Pun (2013).** The suggested method integrated SIFT and local features including color and texture features. And method is robust to complex geometrical transformation such as rotation and scaling in large degree and illumination changes.

L. Li, S. Li and H. Zhu (2013) proposed a technique in which image is first filtered and divided into overlapping circular blocks and then the features of the circular blocks are extracted using rotation invariant uniform local binary patterns (LBP). Feature vectors are obtained and then compared. And the forged regions can be located by tracking the corresponding blocks. This technique is robust in forgery detection, robust to JPEG compression, noise contamination and blurring, rotation and flipping. A deficiency of the proposed method is that when the region is rotated by general angles, it is difficult to detect the forgeries.

R.Davarzani, K.yaghmaie, S.Mozaffari and M.Tapak (2013) proposed a method to detect copy move forgery, in this image is divided into circular block and extracted blocks are filtered using the Wiener filter. Multiresolution LBP features are calculated from sub blocks. Kd tree is used in matching step to reduce the computational cost and Random Sample Consensus (RANSAC) is used to reduce the false positive. This method precisely detects geometric distortion like scaling, rotation, compression, additive noise and blurring.

A method proposed by **Mohammad Farukh Hashmi *et al.* (2013)** is based DWT and SIFT. DWT reduces the image data and obtained the low approximation

coefficients. Robustness was introduced by SIFT. SIFT technique perform well again post image processing, such as additive noise and lossy JPEG compression etc, or even compound processing.

There is a technique based on Discrete Cosine Transformation and Singular Value Decomposition is presented by **J. Zhao *et al.* (2013).** In this method, 2D-DCT is employed to fixed-size overlapping blocks of input image. DCT coefficients are determined for each block. Further, each quantized block is divided into non overlapping sub-blocks and Singular Value Decomposition is used to each sub-block, then features are extracted to minimize the dimension using its greatest singular value. Finally, Lexicography is used to sort the feature vectors, and duplicated image blocks are matched by predefined shift frequency threshold.

Mohamadian and Pouyan (2013) proposed a new method of detecting copy move forgery which is based on SIFT (scale invariant feature transform) algorithm along with the Zernike Moments. SIFT algorithm is used to perform detection but cannot detect flat copied region. This method has one disadvantage of not able to detect flat copy move forgery. To resolve this issue Zernike moments are used.

Sunil Kumar *et al.* (2013) proposed a block matching or block tiling algorithm which was based on Discrete Cosine Transformation (DCT) for detection of copy-move forgery. Time complexity is major challenge in these types of algorithms author successfully addressed this issue by reducing the feature length.

Sunil Kumar *et al.* (2014) proposed a method using PCA on DCT. Firstly DCT is practiced to calculate DCT coefficient for feature extraction and PCA to yield a reduced dimension representation respectively. Features, invariant to local change of intensity are created using down sampling of low frequency DCT coefficients. The method is robust against manipulation techniques like added noise and JPEG compression and also attend invariance to illumination, but it is fails in case of contrast variations.

K. Sudhakar, Sandeep V.M. and Subhash Kulkarni (2014) suggested a new approach to detect Copy Move Forgery using shape signatures derived from distance map. First the image is segmented through geometric deformable model using Chan-

Vese level set method. The distance mapped level set function resulting from segmentation phase is extended to compute the shape descriptors. The method is simple, fast, robust, and efficient as compared to traditional approaches and is invariant to scale, rotation and aspect ratio.

Sondos M. Fad *et al.* (2014) proposed an efficient and fast method to detecting copy move forgery. In this method, accelerate blocking matching strategy by parallel comparing between blocks. First, the tempered image is divided into fixed-size overlapping blocks then calculated features for each block. K-means clustering technique is used to cluster the blocks into different cluster. The feature vectors of each cluster blocks are lexicographically sorted by radix sort, and then a similarity measure is calculated between each nearby blocks. Method is able to detect Copy move and Copy-Rotate-Move forgery.

Forgery Chen-Ming Hsua , Jen-Chun Leeb , and Wei-Kuei Chena (2015) proposed an efficient and robust method to detect copy move forgery. Firstly, Image is divided into overlapping fixed-size block and then Gabor filter is applied to each block of tempered image. Thus statistical features are extracted from the histogram of oriented Gabor magnitude of fixed size overlapping blocks. Finally, feature vectors are sorted lexicographically. Duplicated blocks are identified by finding similar blocks pairs. This method detect multiple copy-move forgery instances, and also robust against slight image rotation, JPEG compression, blurring, brightness adjustment.

Guangcheng Cao, Ying Chen and Gaigai Zong (2015) suggested a method based on the locality preserving projection (LPP) to detect copy-move forgery. Firstly, input image into several small blocks and carry on their coordinates. After that on the premise that the similarity matrix guarantees the adjacent relation unchanged before and after the transformation, LPP algorithm to reduce the small block dimension. Finally, match the reduced dimension of the small blocks to complete the detection. This method can efficiently detect the copy-move forgery quickly and can accurately locate tamper with the position.

Surbhi Sharma *et al.* (2015) proposed a method to detect copy-move in digital images. This method is used to detect copy move forgery detection in medical images using center symmetric local binary pattern (CSLBP) which is able to detect the forgery

size up to 12×12. The method is robust against geometric distortion, Gaussian blurring, JPEG compression and Additive White Gaussian Noise.

Sunil Kumar *et al.* (2015) proposed a method to overcome the limitation .This method was based on binary DCT coefficients. In this method, input image is divided overlapping blocks and DCT is applied to blocks to calculate DCT coefficients. After that binary DCT features are extracted using sign of the DCT coefficients. Coefficient of correlation is used to match resulting binary vectors. This approach is robust against many manipulation techniques such as Gaussian noise addition, compression and minor rotation and scaling.

2.2 Summary

After review I find out that, there are different types of copy-move forgery detection techniques have been suggested for detection of tampering in digital image. Most commonly method is block matching and I found that in the most of the block methods of copy move forgery detection is precise and accurate but the computational cost is very much high. In the literature review, there are many techniques for copy move image forgery, it has been seen that most of the existing block based algorithms use a similar techniques, the only difference is that they apply different feature extraction methods and different matching methods.

Chapter 3 MATERIALS AND METHODS

3.1 Problem Formulation

By study of previous reviews, it was concluded that, there are different types of copy-move forgery. Copy-Move forgery is to detect image areas that are same or extremely similar. Copy move image forgery detection is utilized to figure out the replicated regions as well as the pasted parts And I find that in most of the block based methods of copy move forgery detection is precise and accurate but the computational cost is very much high. I studied about existing copy move image forgery detection approaches. After studying the literature I find that the matter of time complexity in the field of image forgery (just copy move) detection.

3.2 Research Methodology

Research methodology implies simply the method that is intended to use in our work. It can be used for resolving problems and better implementation of the research work. The research activities that were followed consisted of following phases that are depicted in figure 3.1.

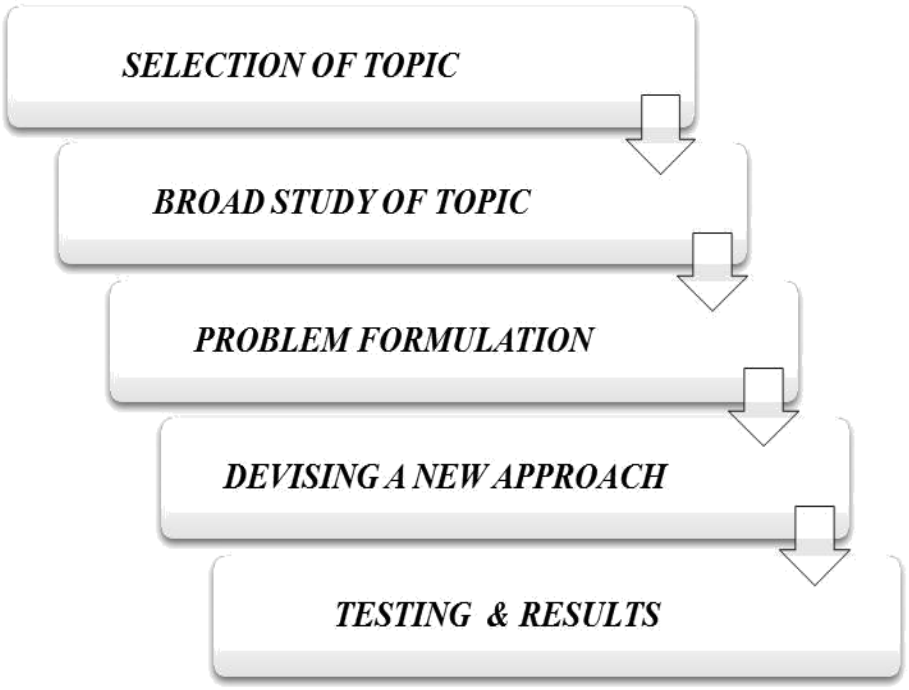


Figure 3.1: Research Methodology

Selection of Topic:

The first phase of my work starts with the selection of dissertation topic. Digital image forgery means the purposely manipulation of digital image, for the purpose of altering the semantic meaning of the visual message included in that image. Image forgery detection is a very popular and sophisticated research topic nowadays, because of the importance and impact that it has on our social behavior. Due to the expansion in technology of digital image, and availability of low-cost hardware and software editing tools, Digital images are susceptible in the sense that, it can be effortlessly manipulate to hide or alter the meaning.

Literature Review:

In the second phase of dissertation, I have done a broad study of topic. In the literature review, Most commonly method is block matching and I found that in the most of the block methods of copy move forgery detection is precise and accurate but the computational cost is very much high. There are many techniques for copy move image forgery, it has been seen that most of the existing block based algorithms use a similar techniques, the only difference is that they apply different feature extraction methods and different matching techniques. Improvement in term of time complexity of detection of copy move forgery is the most important concern in Image forgery.

Problem Formulation:

By study of previous reviews, it was concluded that, there are different types of copy-move forgery. Copy-Move forgery is to detect image areas that are same or extremely similar. Copy move image forgery detection is utilized to figure out the replicated regions as well as the pasted parts And I find that in most of the block based methods of copy move forgery detection is precise and accurate but the computational cost is very much high. I studied about existing copy move image forgery detection approaches. After studying the literature I find that the matter of time complexity in the field of image forgery (just copy move) detection.

Developing new approach:

Fourth phase is divided into two parts. In the first part I created the simulation environment in my system. For this I first installed MATLAB R2013a. After this I learned how to work with tool.

In the second part of the fourth phase I proceeded with the design of my proposed model. So while designing the proposed model I have to keep in mind time complexity have to be reduce in proposed model.

Testing & Results:

In the final phase based on the result of the fifth phase I have written the conclusion of my dissertation which explains the comparison result that I have got. Then I discussed my conclusion with my mentor.

3.3 Tools Used

- Matlab 8.1.0.604 (R2013a)

3.3.1 MATLAB

Simulation is the process of implementing a real world process in a virtual environment. The action of simulating something firstly needs a model to be developed; then this model presents the key features or behaviors of the selected process. The simulation proposes the working of the system over time whereas the model represents the system itself. The issues with simulation include attainment of validation of the source information about the section that is relevant for the key features and behaviors.

In this dissertation a simulation environment is needed to perform the analysis and acquire the result. To perform the calculation, a mathematical program is needed. MATLAB is selected due to its capability to perform numerical computation in an effective manner.

The name MATLAB stands for MATrix LABoratory. MATLAB (matrix laboratory) is fourth generation high level programming language & interactive environment for numerical computation, Visualization and programming. MathWorks is the developer of MATLAB. It allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python. MATLAB also has some tool boxes useful for signal processing, image processing, optimization, etc. Typical uses include:

- ✓ Math and computation.
- ✓ Algorithm development.

- ✓ Modeling, simulation, and prototyping.
- ✓ Data analysis, exploration, and visualization.
- ✓ Scientific and engineering graphics.
- ✓ Application development, including Graphical User Interface building.

3.4 System Requirements

The algorithm is implemented in MATLAB R2013a programming tools on a PC with Windows 7 and the following features:

- ✓ Processor: Intel(R) Core(TM) i3-3110M CPU @ 2.40 GHz 2.40 GHz
- ✓ Installed Memory (RAM): 2.00 GB
- ✓ System Type: 64-bit operating system

3.5 Proposed Work Description

In this thesis work, I address the issue of computational complexity in the field of image forgery (just copy move) detection. Copy-move forgery is cover, remove or add specific object in image, as a result there are two similar regions in image. Copy-move forgery detection is to find image areas that are same or extremely similar.

For detection of image forgery, perform a particular series of operations on image. In this passive technique takes every image as a forged or tampered image. After we go through a particular series of operations image is categorized into two categories: authentic images and forged images. Here I describe here a typical procedure of passive detection techniques of digital image forgery has been followed as shown in Figure 3.2

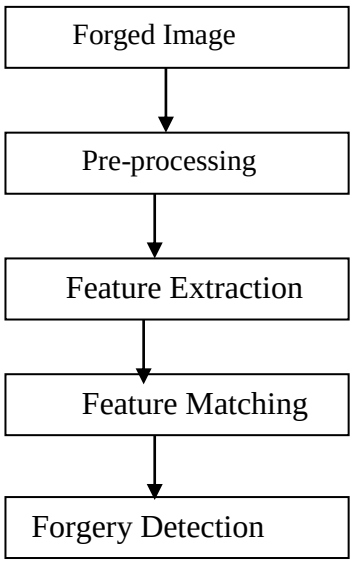


Figure 3.2: Block diagram of Copy-move forgery detection algorithm.

1. **Image preprocessing:** This is the first step of copy move forgery detection technique.

   In this step inputted the color image and then convert it to grayscale image. Then this grayscale image is of dimension of m x n is decomposes into number of overlapping blocks of b x b pixels in dimension. Copy Move Forgery Detection method can either block based and keypoint based approach. Block based method- In this method, the suspected image is divided into overlapping blocks & then makes a comparison in blocks to detect duplicated region. Key point-based methods operate on whole image. Instead block based methods, Key point based methods compute their features only on image regions with high entropy. One of the most frequently used methods to detect such type of forgery is to use block based method. Most of the time in block based method needs gray scale images.

2. **Feature extraction:** feature is extracted after pre-processing step. It is the process of finding a new representation of the data (image) in terms of features. The main aim of this step is to extract discriminate features that represent the data well. Avoiding redundancy and reducing the dimensionality of the data are two requirements for good features.

3. **Matching:** After feature extraction, detection of the copy move forgery method looking for the similar blocks. In this step feature are matched to obtain duplicated regions in suspected image. Now is the point at which determining the duplicated block of inputted suspicious image based on their features.

4. **Forgery Detection:** In this final step of detection of duplicated region in the suspected image, the algorithm outputs a black map image; regions which are taken as duplicated region are marked with a black color.

3.6.1 Proposed Algorithm

Because of the nature of copy-move forgery, there is duplicate region is detected in a digital image then that image is considered as copy-move tampered. We suppose that the duplicated region is non-overlapping. The main task of the technique is to

effectively and efficiently determine whether an image contains duplicated regions or not. Since the size and shape of duplicated regions are non-regular so, it is impossible to computationally examine every possible pairs of regions. Block based methods are good at detecting the tampered region with high accuracy but are having high computational complexity. However, block based method is more effective and efficient approach in order to determine the duplicated region in the suspected image.

In this thesis work, the issue of time complexity of detection algorithm is addressed and the experimental results show that the performance of method has improved in terms of execution time.

Feature extraction is the process of finding a new representation of the data (image) in terms of features. The key idea is to extract discriminate features that represent the data well. Avoiding redundancy and reducing the dimensionality of the data are two requirements for good features.

Principal Component Analysis (PCA):

Here, the Principal Component Analysis (PCA) is applied to extract features of suspected image. PCA is a mathematical procedure used in reduction of data dimension. It converts correlated variable to linearly related variable called principal component.PCA reduce and eliminate the redundant features of the image. In particular it neatly summarizes all correlations in your data. Usually there are amount of correlation between different dimensions of raw input data. Actually the PCA rotates the coordinate system in such a way that the new dimensions are completely uncorrelated and represent different and independent aspects of the input data. PCA assigns a score to each dimension which declares the variance of data over that dimension. Those dimensions which have the highest variance have the highest information to represent the data, because the low variance dimensions are mapping all the data into a closed region and are not able to discriminate data samples from each other. Main advantage of PCA is data compression without much loss of information. Thus PCA is a procedure that allows reduction of dimension without much sacrificing the accuracy.

Algorithm:

- Compute the covariance matrix of the dimensions

(Covariance calculations are used to find relationships between dimensions in high dimensional data sets)

Covariance Matrix: Representing covariance among dimensions as a matrix

- Find eigenvectors of covariance matrix
- Sort eigenvectors in decreasing order of eigenvalues
- Project onto eigenvectors in order

3.6.2 Algorithm Framework

The proposed algorithm based on PCA is presented below. Aim is to find the image areas that are same or extremely similar. Methods for detecting the Copy-Move Forgery can be divided into four steps. Details are as follows:

Step 1: Converting the colored image into grayscale image:

The inputted the suspected image of size m x n, we assuming this is grayscale image. If this image is not grayscale image convert this to grayscale image from RGB color image by the luminosity method: I = 0.228R + 0.587G + 0.114B**.** To reduce the time complexity of overall algorithm, we use grayscale image.

Where R, G, B are Red, Green and Blue bands.

Colored Image **Grayscale Image**

Step 2: Feature Extraction (PCA):

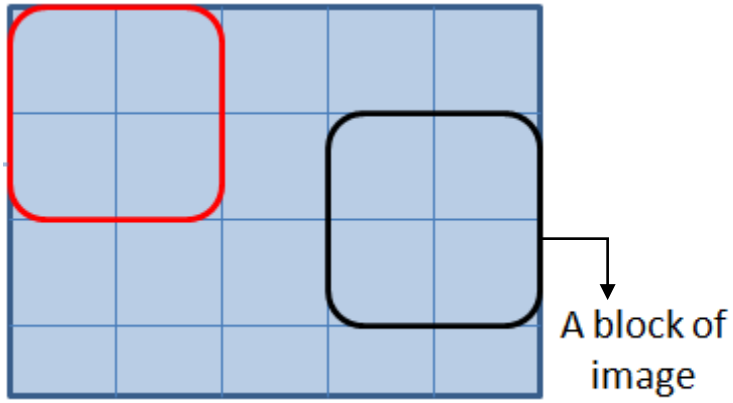
- Feature extraction is a process of taking out informative and non-redundant data from the image. PCA or Principal component analysis is a type of feature extraction process which deals in bringing out strong patterns in a dataset.

- Feature extraction is a type of dimensionality reduction that efficiently represents interesting parts of an image.

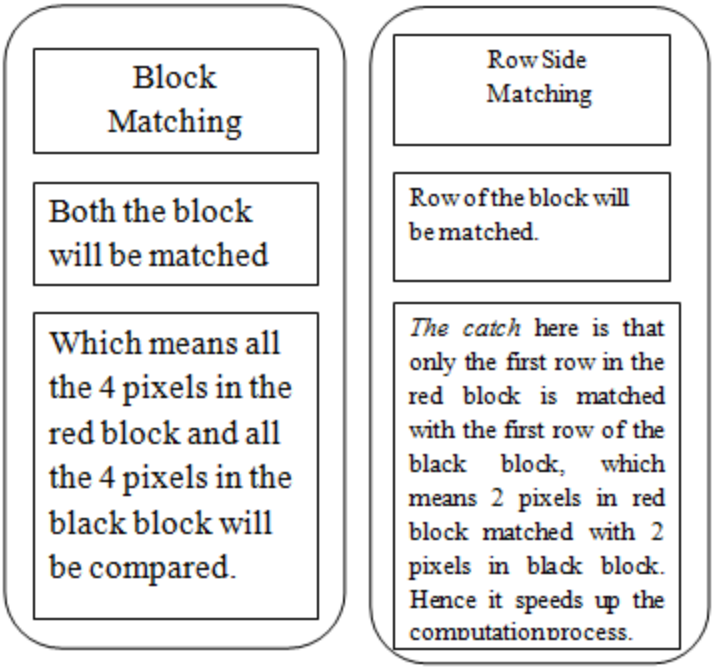
  PCA is applied on the grayscale image to reduce the dimension of grayscale image.

Step 3: Dividing image into blocks & Side-matching technique

Image is divided into blocks with an initial size of 2 * 2 which keeps on increasing with a multiple of 2 (i.e. 4*4, 8*8 etc.). These blocks are then compared using side matching technique which is a successor of block matching technique. In this technique we instead of matching the entire block of image, we compare either the row side or the column side of the image. Each block is compared and their standard deviation is stored in an array. These standard deviation values are then compared with each other. The lowest standard deviation value will be the duplicate/forged region.



An Image of m rows and n column



Old Algorithm **New Algorithm**

Here we are comparing each of block by using side matching technique. Calculate Standard deviation corresponding to compared blocks using side matching technique. First calculate mean and variance then standard deviation for compared blocks**.** Let suppose we have 2 x 2 block has to be compared with other 2 x 2.Here in this case taking only one row of the block i.e. only two variable for one block.

Calculation of standard deviation:

For $Q_i = (B_{i1}, B_{i2}.....B_{in})$

And $Q_{i+j} = (B_{i+j1}, B_{i+j2}.....B_{i+jn})$

Computing mean and variance of Q_i ,Q_{i+J} is described as follows:

Now mean is represented by M and total number of element is N. Standard deviation is:

$$\boldsymbol{\sigma = \sqrt{\frac{\sum(i-M)^2}{N}}}$$

Now standard deviation has been calculated for comparing block. Repeatedly, this process is applied to all the block of image. The blocks which have lowest standard deviation considered as forged blocks.

Step 4: Highlight the blocks that shows repetition

Those regions that show the repetition must be highlighted in such a way that the forged/tampered area is visible to human eye. This is the last step of the algorithm, in

this step both, the original and duplicated region are marked with black color in order to highlight the forged region. The block diagram of the algorithm is shown in figure 3.4 given below:

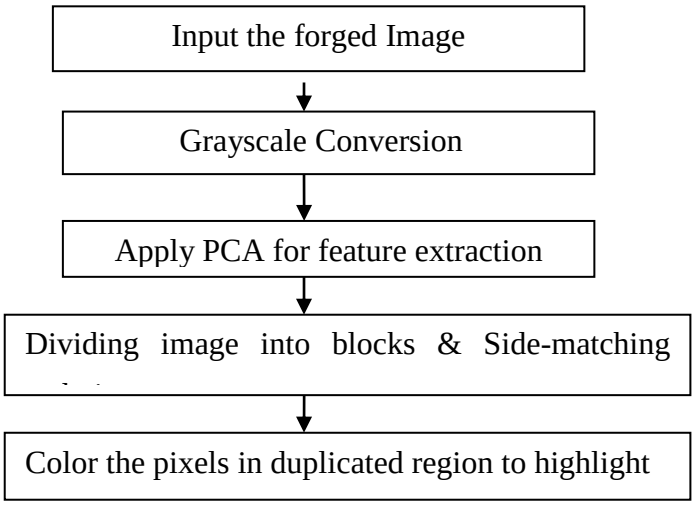
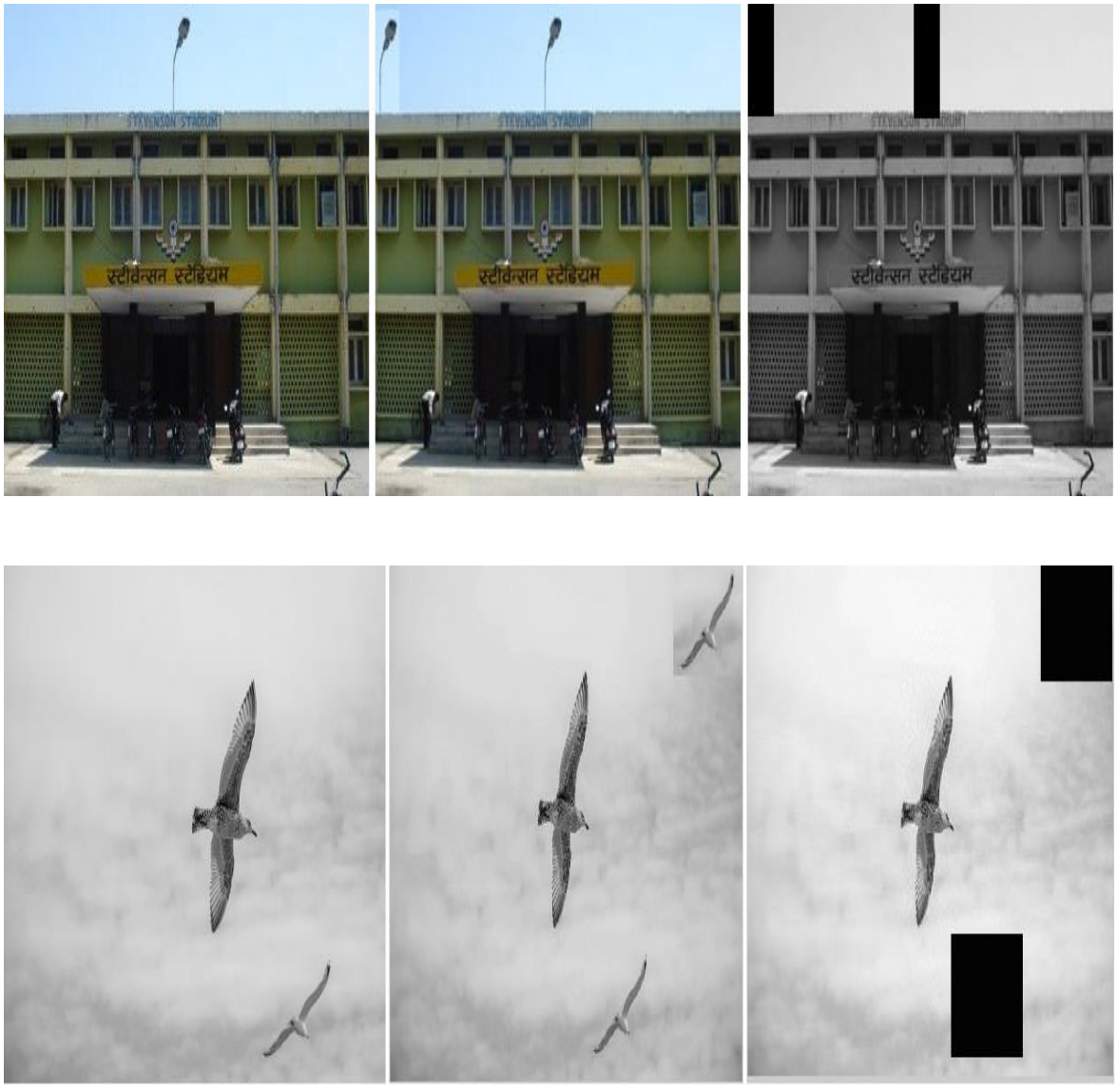


Fig.3.4 Flow chart of proposed algorithm

Chapter 4 RESULTS AND DISCUSSION

4.1 Visual Results

This experiment is designed to validate the proposed method for the copy-move forgery. In experiment, we first tampered tested images by copying its part content and pasting somewhere else in the image, and then detected tampered images by using one method. Fig.4.1 shows the experimental results, the duplicated regions can be detected.



(a)Original images (b) Forged images (c) Forgery Detection

Fig.4.1 Visual result to show Copy-Move Forgery Detection.

4.2 Efficiency Testing

In order to test the efficiency of the proposed method, we tested the detection time. In experimental, tested images are different in size and their type is JPEG. Table 4.1 shows statistical average values of the time cost.

Image size	128x128	256x256	384x 384	424 x424	512 x512	656 x656	832 x832
Detection time (s)	9.098	10.243	12.168	14.714	20.981	44.653	50.421

Table 4.1 Time taken to detect copy move forgery

4.3 Image set

Dataset of four different types (low resolution, high resolution, low contrast, and high-contrast) of images is used. And tested images are of JPEG type. Proposed method is compared with other related method namely F_DCT that is proposed by **Sunil *et al.* (2013).**

4.4 Experimental results for low contrast images

Fig 4.2 shows an example of copy-move forgery in a low contrast image. A low contrast image is a type of image in which the color of background and foreground objects is almost same. The original image, Forged image and the image after forgery detection are represented by Fig. 4.2 (a), (b), and (c) respectively. Fig. 4.3 shows the comparison execution time F_DCT and proposed method.

(a) Original image (b)Forged image (c) Forgery Detection

Fig. 4.2 copy-move forgery in a low contrast image (256x256)

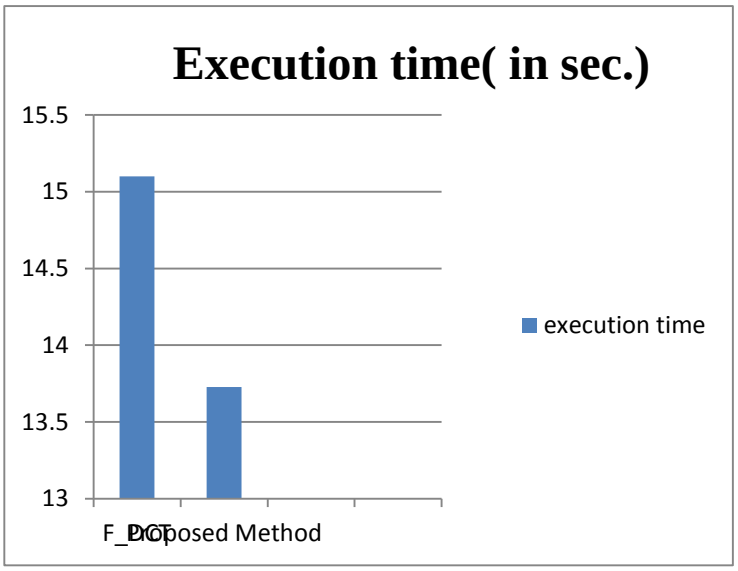


Fig. 4.3 Comparison of execution time for low contrast image

The proposed method detects simple copy-move forgery with lower execution time as compared to F_DCT.

4.5 Experimental results for high contrast image

Fig 4.4 shows an example of copy-move forgery in a high contrast image. A high contrast image is a type of image in which the color of background and foreground objects is very different. The original image, Forged image and the image after forgery detection are represented by Fig. 4.4 (a), (b), and (c) respectively. Fig. 4.5 shows the comparison execution time of F_DCT and proposed method.

(a) Original image (b)Forged image (c) Forgery Detection

Fig. 4.4 copy-move forgery in a high contrast image (256x256)

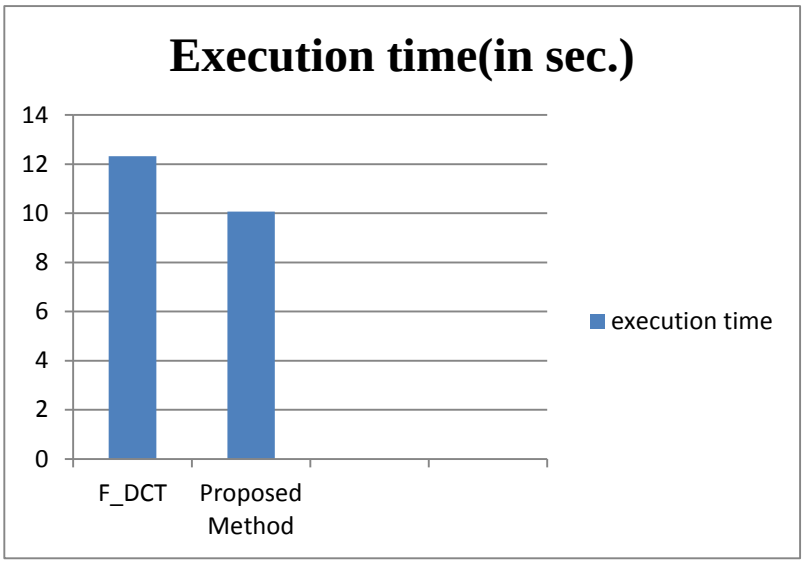


Fig. 4.5 Comparison of execution time for high contrast image

The proposed method detects simple copy-move forgery with lower execution time as compared to F_DCT.

4.6 Experimental results for low resolution image

Fig 4.6 shows an example of copy-move forgery in a low resolution image. The original image, Forged image and the image after forgery detection are represent4.6 (a), (b), and (c) respectively. Fig. 4.7 shows the comparison execution time of F_DCT and proposed method.

(a) Original image (b)Forged image (c) Forgery Detection

Fig. 4.6 copy-move forgery in a low resolution image (256x256)

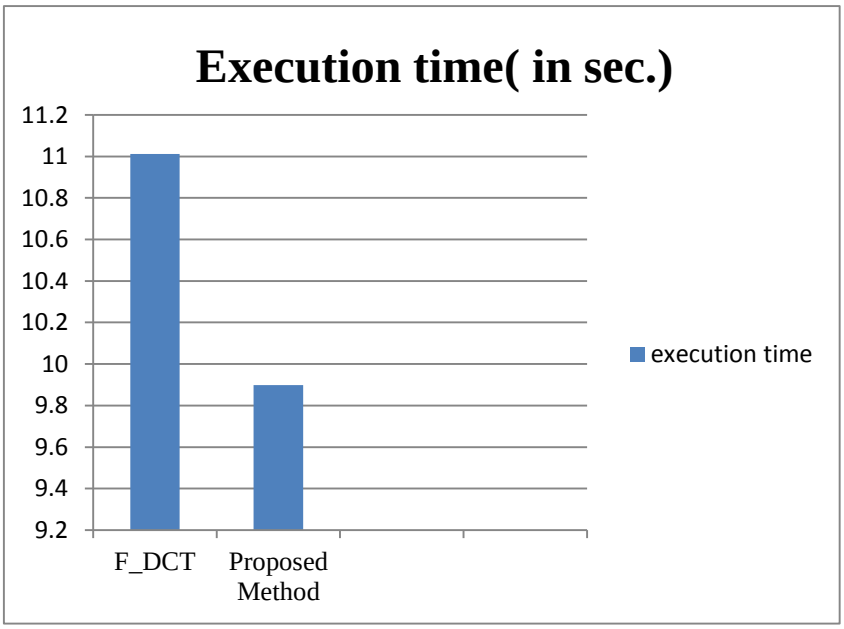


Fig. 4.7 Comparison of execution time for low resolution image

The proposed method detects simple copy-move forgery with lower execution time as compared to F_DCT.

4.7 Experimental results for high resolution image

Fig 4.8 shows an example of copy-move forgery in a high resolution image. The original image, Forged image and the image after forgery detection are represented by Fig. 4.8 (a), (b), and (c) respectively. Fig. 4.9 shows the comparison execution time F_DCT and proposed method.

(a) Original image (b)Forged image (c) Forgery Detection

Fig. 4.8 copy-move forgery in a high resolution image(600x533)

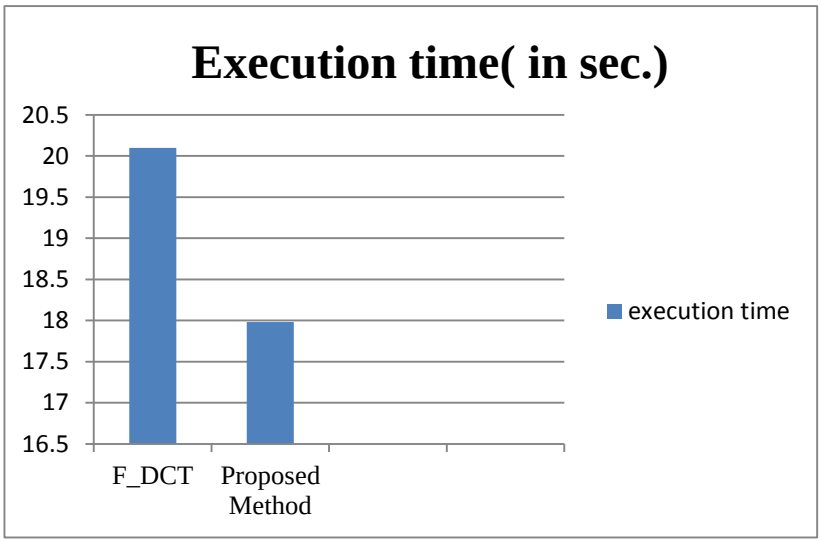


Fig. 4.9 Comparison of execution time for high resolution image

The proposed method detects simple copy-move forgery with lower execution time as compared to F_DCT.

4.8 Comparison table for execution time

In a nutshell, now we can summarize all above discussed results in a tabular form as shown in the Table 4.2

Name of Image	Running Time (in sec.) of F_DCT Method	Running Time (in sec.) of Proposed Method
Image 1(Low Contrast)	15.10	13.728
Image 2(High Contrast)	12.32	10.063
Image 3(Low Resolution)	11.012	9.898
Image 4(High Resolution)	26.768	20.57

Table 4.2 Comparison table for execution time of F_DCT and proposed method

The above comparison shows that the proposed method is far better than the existing method proposed by **Sunil *et al.* (2013)**.

To compare the speed of the proposed algorithm with the existing method, a database of more than 50 images is developed. The database consists of images with different contrasts and resolutions.

In the first case, a low contrast image is shown in Fig. 4.2. In this image the forgery is created in this image. The proposed method successfully locates the copied and the pasted region and colors both of them as black to highlight it. The graph created in the Fig. 4.2 shows the comparison of the DCT and F_DCT with the proposed method. In Fig. 4.3 a high contrast image, in Fig. 4.5 a low resolution image and in Fig. 4.7 a high resolution image is shown and in Fig. 4.4, 4.6 and 4.8 the comparison result of corresponding image's computational time is represented. It revealed that the proposed method is faster than the existing methods. Thus, the proposed algorithm is the improved version of the block matching algorithms.

The proposed method detected the forgery with lower execution time. Also the efficiency of the proposed method is highly dependent upon the size of copy-moved region

Chapter 5 SUMMARY AND CONCLUSIONS

5.1 Summary

This thesis gives a description of various existing copy move forgery detection techniques with a literature survey and provides a description for working of detection of copy move forgery.

Block matching technique is most commonly used technique to detect the duplication in the digital image. As the image size increases the time complexity to detect the duplicated region takes relatively long time. One of the major challenges is the time complexity of such algorithms.

In this thesis work, I address the issue of time complexity in the field of image forgery and proposed an improved digital image forgery detection method in term of lower execution time. In proposed method, Principal Component Analysis (PCA) has been used to extract features of suspected image. PCA is a mathematical procedure used in reduction of data dimension. Main advantage of PCA is data compression without much loss of information. Then this image is divided into blocks. Initially the block size is 2x2 which keeps on increasing with a multiple of 2 (i.e. 4*4, 8*8 etc.). These blocks are then compared using side matching technique which is a successor of block matching technique. Thus this proposed algorithm reduces the time complexity of detecting copy-move forgery in digital image.

5.2 Conclusion

The proposed method is evaluated on a number of original and forged images. According to experimental results the proposed method is quite attractive in comparison to previous method. The copy-move forgery is done with low contrast images, high contrast images, low resolution images and high resolution images. In this process, an image database that consists of original and forged images is also created.

The proposed method detects efficiently copy-move forgery (just copy-move) without post processing operations such as scaling rotation, reflection, noise addition and JPEG compression.

We also created a database consisting of more than 50 images. These

images are forged with different types of copy-move, and added to the database.

5.3 Future Scope

According to the performance of the proposed method to detect copy-move forgery in digital images, in future, the following improvements can be done:

1. The accuracy of forgery detection for the rotation and scaling may be studied further.
2. The accuracy of forgery detection for added random noise and JPEG compression may be studied further.

LITERATURE CITED

Ashwin, S., Min Wu. 2008. Digital Image Forensics via Intrinsic Fingerprints. *Transaction on Information Forensics and Security.* IEEE 3(1), 101-117

Bashar, M. , Noda, K. Ohnishi , N. and Mori, K. 2010. Exploring duplicated regions in natural images. IEEE Trans Image Process. 1–40.

Bayram, S. Sencar, H.T. Memon, N. 2009. An efficient and robust method for detecting copy- move forgery**.** *In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing.*1053–1056.

Bo Liu and Chi-Man Pun .2013. A SIFT and Local Features Based Integrated Method for Copy-Move Attack Detection in Digital Image**.** *Proceeding of the IEEE International Conference on Information and Automation Yinchuan, China.*

Bo Xu, Guangjie Liu and Yuewei Dai.**2012.**A Fast Image Copy-move Forgery Detection method using Phase Correlation **.** *IEEE Fourth International Conference on Multimedia Information Networking and Security.*

Bravo-Solorio, S. & Nandi, A. K. 2011. Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics . *Signal Processing,* 91(8), 1759-1770.

Cao, G., Chen, Y. Zong, G. 2015. Detection of Copy-move Forgery in Digital Image Using Locality Preserving Projections .IEEE *8th International Congress on Image and Signal Processing* .

Cao, Y. Gao, T. Fan, L. and Yang, Q .2012. A robust detection algorithm for copy-move forgery in digital images. *Forensic science international.* 214, 33-43.

Davarzabi, R. Yaghmaie, K. Mozaffari, S. and M.Tapak, M. 2013. Copy-move forgery detection using multiresolution local binary patterns. *Forensic science international.* 231, 61-72.

Dybala, B. Jennings, B. Letscher, D.2007. Detecting filtered cloning in digital images**.** *MM&Sec'07: Proceedings of the 9th Workshop on Multimedia & Security, ACM, New York, NY, USA.*43–50

Forgery Chen-Ming Hsua , Jen-Chun Leeb , and Wei-Kuei Chena. 2015. An Efficient detection algorithm for Copy-Move**.** *IEEE 10th Asia Joint Conference on Information Security.*

Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. 2003. Detection of copy-move forgery in digital images . *In Proceedings of Digital Forensic Research Workshop.*

Ghorbani, M. Firouzmand, M. and Faraahi, A .2011. DWT-DCT (QCD) based copy-move image forgery detection**.** *in 18th IEEE International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 14*.

Huang, H., Guo, W. and Zhang, Y.2008. Detection of copy-move forgery in digital images usingSIFT algorithm. *Proceedings of the Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Volume 2, December 19-20, Wuhan, China.* 272-276.

Huang, Y. Lu, W. Sun, W. and Long, D. 2011. Improved DCT-based detection of copy-move forgery in images**.** *Forensic science international.*206, 178-184.

Jie Hu . 2013. An Improved Lexicographical Sort Algorithm of Copy-Move Forgery Detection.*Second International Conference on Networking and Distributed Computing*

Judith, A. R. Wiem, T. Jean-Luc, D. 2010. Digital image forensics: a booklet for beginners.*Multimedia Tools and Applications.*51, 133-162.

Kakar, P. and Sudha, N. 2012. Exposing Postprocessed Copy-Paste Forgeries Through Transform-Invariant Features. *Information forensic and security, IEEE transaction on*, 7,1018-1028.

Kang, L. and Cheng. X.-P. 2010. Copy-move forgery detection in digital image. *in 3rd International Congress on Image and Signal Processing.* IEEE *Computer Society*, 2419_21.

Kang, X. and Wei, S. 2008. Identifying tampered regions using singular value decomposition in digital image forensics. *in: Proceedings of International Conference on Com-puter Science and Software Engineering.*926–930.

Khan, S. and Kulkarni, A. 2010. Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform. *International Journal of Computer Applications.* 6(6), 31-36.

Kumar, S. Das, P.K. 2011. Copy-Move Forgery Detection in Digital Images: Progress and Challenges .*International Journal on Computer Science and Engineering (IJCSE),* 3, 652-663

Kumar, S. Desai, J. and Mukherjee, S.2014. DCT-PCA based method for copy-move forgery detection. *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing.*

Kumar, S. Desai, J. and Mukherjee, S.2015. Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors. *International Journal of Image,Graphics and Signal Processing (IJIGSP)* 7(6) 38.

Leida, Li .2012. Copy-Move Forgery Detection Based on PHT. *World Congress on Information and Communication Technologies.*

Li, G. Wu, Q. Tu, D. Sun, S. 2007. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. *International conference on multimedia & Expo*, 1750–3.

Lin, H.-J. Wang, C.-W. & Kao, Y.-T. 2009. Fast copy-move forgery detection. *WSEAS Transactions on Signal Processing, 5(5), 188-197.*

Li, L., Li, S., & Wang, J. 2012. Copy-move forgery detection based on PHT **.** *Paper presented at the Information and Communication Technologies (WICT), World Congress on*

Li, L. Li, S. and Zhu, H. 2013. An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns. *Journal of Information hiding and Multimedia Signal Processing.*4, 46-56.

Lin, S.D .2011. An Integrated Technique for Splicing and Copy Move Forgery Image Detection. *in IEEE 4th International Congress on Image and Signal Processing (CISP),* 2,1086-90.

Luo, W. Huang, J. & Qiu, G. 2006. Robust detection of region-duplication forgery in digital image. *Paper presented at the Pattern Recognition, ICPR 18th International Conference on.*

Mahdian, B. and Saic , S. 2007. Detection of copy-move forgery using a method based on blur moment invariants **.** *Elsevier Forensic Science International,* 171(2),180-189

Minakshi. 2003. Digital Image Processing. *Satellite Remote Sensing and GIS Applications in Agricultural Meteorology,* 81-102

Mohamadian, Z., & Pouyan, A. A. 2013. Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions. *Paper presented at the UKSim.*

Motasem AlSawadi .2013. Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering. *European Modelling Symposium*

Mohammad Farukh Hashmi, Aaditya R. Hambarde and Avinash G. Keskar .2013.

Copy move forgery detection using DWT and SIFT features. *13th International Conference on Intelligent Systems Design and Applications (ISDA),* IEEE , 188-193.

Muhammad, G., Hussain, M. Khawaji, K. Bebis, G. 2011. Blind copy move image forgery detection using dyadic undecimated wavelet transform. *In: Proc. 17th digital signal processing (DSP) conference, Corfu, Greece; July.*

Muhammad, G. and Hossain, M.S. 2011. Robust copy-move image forgery detection using undecimated wavelets and Zernike moments. *in Proceedings of the Third International Conference on Internet Multimedia Computing and Service,* 2011, 95-98.

Muhammad, H. , Muhammad, G. 2012. Copy-move image forgery detection using multi-resolution weber descriptos. *Eighth International Conference on Signal Image Technology and Internet Based Systems.* IEEE.

Myna, A.Venkateshmurthy, A. Patil, M**. 2007.** Detection of region duplication forgery in digital images using wavelets and log-polar mapping. *The International conference on computational intelligence and multimedia applications (ICCIMA),* 371–7.

Nguyen HC, Katzenbeisser S. 2012. Detection of copy-move forgery in digital images using radon transformation and phase correlation. *Proceedings of the 8th International Intelligent Information Hiding and Multimedia Signal Processing* IEEE, 134–137.

Popescu, A. Farid H. 2004. Exposing digital forgeries by detecting duplicated image regions. *Technical Report TR2004-515. Department of Computer Science, Dartmouth College.*

Ryu, S.-jin, Lee, M.-jeong and Lee, H.-kyu .2010. Detection of copy-rotate- move forgery using zernike moments**.** *IH , LNCS* 6387, 1, 51-65.

Sevinc, B. Husrev, T. S. Nasir, M. 2008. *A Survey of Copy Move Forgery Detection Techniques*. IEEE Western New York Image Processing Workshop.

Sharma, S. 2013. A Fast DCT Based Method for Copy Move ForgeryDetection. Proceeding of the Second International Conference on Image Information Processing.

Sharma, S. 2015. A rotationally invariant texture descriptor to detect copy move forgery in medical images**.** *International Conference on Computational Intelligence & Communication Technology.* IEEE.

Sondos M. Fad .2014. Copy-rotate-move forgery detection based on spatial domain. *Computer Engineering & Systems (ICCES), 9th International Conference on.*

Sridevi, M., Mala, C., & Sandeep, S. 2012. Copy–move image forgery detection in a parallel Environment. *Computer Science & Information Technology (CS & IT)*, 52, 19-29.

Sudhakar, K. Sandeep, V.M. and Kulkarni, S. 2014. Shape Based Copy Move Forgery Detection Using Level Set Approach. *Fifth International Conference on Signals and Image Processing. IEEE*

Ting, Z., & Rang-ding, W. 2009. Copy-move forgery detection based on SVD in digital image. *Paper presented at the Image and Signal Processing. CISP'09. 2nd International Congress on.*

Wang, J.-W., Liu, G.-J., Zhang, Z., Dai, Y., & Wang, Z. 2009. Fast and robust forensics for image region duplication forgery. *Acta Automatica Sinica*, 35(12), 1488- 1495.

Wang, J., Liu, G., Li, H., Dai, Y., & Wang, Z. 2009. Detection of image region duplication forgery using model with circle block. *Paper presented at the Multimedia Information Networking and Security, International Conference on.*

Zhang, J. Feng, Z. and Su, Y.2008. A new approach for detecting copy-move forgery in digital images. *International Conference on Communication Systems, China,* IEEE 362_6.

Zhao, J. Guo, J. 2013. Passive forensics for copy-move image forgery using a method based on DCT and SVD..*Forensic Science International*. 233(1–3):158–166.

Zimba, M. Xingming, S. 2011. DWT-PCA (EVD) based copy-move image forgery detection. *Int. J. Digital Content Technol.* 5 (1) 251–258.

Zimba, M. and Xingming, S. 2011. Fast and robust image cloning detection using block characteristics of DWT coefficients. *JDCTA: International Journal of Digital Content Technology and its Applications*.

VITA

The author, Rachana was born on July 31, 1991 at Rishikesh, Uttarakhand. She passed her High School from GGIC, Rishikesh and Intermediate from GGIC, Rishikesh from State Board of Uttarakhand, during the year 2006 and 2008, respectively. She completed her B. Tech. Degree in Computer Science & Engineering in 2012 from Uttaranchal Institute of Technology, Dehradun, affiliated to Uttarakhand Technical University.

She joined as a Non-Gate Candidate in Govind Ballabh Pant University of Agriculture & Technology, Pantnagar for her post Graduate Programme (Master of Technology) with major in Information Technology in 2014.

Address:

Rachana

D/O Mr. Jagdish Prasad

Vill-Rishikesh

Post-Rishikesh

Dehradun (Uttarakhand)

PIN (249201)

E-mail rachana1416@gmail.com

Contact (+91) – 8057801324

ABSTRACT

Name	**: Rachana**	**Id. No.**	**: 48177**
Semester & Year of admission	**: 1st, 2014-2015**	**Degree**	**: Master of Technology**
Major	**: Information Technology**	**Department**	**: Information Technology**

Thesis Title : **Study and Analysis of Copy-Move Forgery Detection in Digital image using MATLAB**

Advisor : **Mr. Ashok Kumar**

With the rapid development of ubiquitous availability of imaging tools and software, it is not difficult to tamper or forge the digital image. As a result, digital images can no longer be trusted. Therefore each and every digital image must therefore be subject to test for authenticity in many areas-forensic investigation, criminal investigation, surveillance system, intelligent system, medical imaging and journalism. Digital Image Forensic is rising and swiftly growing field of image processing area to find the authenticity of digital image. Copy-Move attack is very common type of tampering technique, where a part of an image is copied and pasted elsewhere in the same image to conceal a special object in the original image. Many block based methods have been suggested to detect duplicated region (Copy-Move forgery).One of the major challenge of these block based is the time complexity. As the image size increases the execution time of such algorithm is also increases. In the proposed method, PCA is applied to the suspected image to reduce its dimensionality. Thus, Principal Component Analysis is for digital image compression. I have devised and implemented a side matching approach to reduce the time complexity. This proposed algorithm improves the time complexity in detection of Copy-Move Forgery.

(Ashok Kumar)
Advisor

Rachana
(Rachana)
Authoress

सारांश

नाम : रचना परिचयाक : ४८१७७

प्रवेश का सत्र एवं वर्ष: प्रथम षट्मास २०१४-२०१5 उपाधि : स्नातकोत्तर अभियांत्रिकी

मुख्य विषयशोध : सूचना प्रोधोगिकी विभाग : सूचना प्रोधोगिकी

सलाहकार : अशोक कुमार

शोधग्रंथ का शीर्षक : मैटलैब का उपयोग कर डिजिटल छवि में कॉपी-मूव जालसाजी का अध्ययन और विश्लेषन

इमेजिंग उपकरण और सॉफ्टवेयर की सर्वव्यापक उपलब्धता के तेजी से विकास के साथ, डिजिटल छवि मे बदलाव या छेड़छाड़ करना अब मुश्किल नहीं रह गया है। नतीजतन, डिजिटल छवियों पर कोई भरोसा नही किया जा सकता है। इसलिए हर एक डिजिटल छवि कि प्रामाणिकता, परीक्षण के अधीन होना चाहिए जिसका ऊपयोग कई क्षेत्रों मे जैसे - फोरेंसिक जांच, आपराधिक जांच, निगरानी प्रणाली, बुद्धिमान प्रणाली, मेडिकल इमेजिंग और पत्रकारिता मे हो सके। डिजिटल छवि फोरेंसिक का ऊपयोग बढ़ रहा है और तेजी से डिजिटल छवि की प्रामाणिकता खोजने के लिए छवि प्रसंस्करण के क्षेत्र मे आगे बढ़ रहा है। कॉपी-मूव हमला बहुत ही आम प्रकार कि छेड़छाड़ तकनीक है , जिसमें एक छवि के एक हिस्से की नकल करके एक ही छवि के किसी अन्य स्थान में चिपकाया जाता है जिससे एक विशेष वस्तु को छुपाया जा सके। दोहराए क्षेत्रो (कॉपी-मूभ जालसाजी) का पता लगाने के लिए कई ब्लॉक आधारित विधियों का सुझाव दिया गया है। कॉपी- मूव जालसाजी का पता लगाने वाली एल्गोरिथ्म की सबसे बड़ी चुनौती समय कि जटिलता है। छवि का आकार जिस तरह से बढता है ऊसी रूप से एल्गोरिथ्म के निष्पादन का समय भी बढ़ जाता है। प्रस्तावित विधि में, पीसीए संदिग्ध छवि के लिए लागू किया जाता है। इस प्रकार, पीसीए डिजिटल छवि संपीड़न के लिए है। मैने side matching को समय जटिलता को कम करने के लिये कार्यान्वित किया है। यह प्रस्तावित एल्गोरिथ्म कॉपी- हटो जालसाजी का पता लगाने में समय जटिलता को बेहतर बनाता है। इस शोध का लक्ष्य कॉपी- मूव जालसाजी का पता लगाने के एल्गोरिथ्म के प्रदर्शन में सुधार करना है। इस प्रस्तावित एल्गोरिथ्म से कॉपी-मूव जालसाजी का पता लगाने के निष्पादन के समय में सुधार करना है।

(अशोक कुमार)
सलाहकार

Rachana
(रचना)
शोधकर्ता

Paper Published

Rachana, Ashok Kumar, H.L. Mandoria, Binay Pandey "Study and Analysis of Copy-Move Forgery Detection in Digital Image: A Review**"** published in International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 03 Issue: 05, May-2016.

Rachana, Ashok Kumar, H.L. Mandoria, Binay Pandey "Study and Analysis of Copy-Move Forgery Detection Forgery in Digital Image Using MATLAB" published in International Journal for Research in Applied Science Engineering and Technology (IJRASET) e-ISSN: Volume: 04 Issue VIII (August 2016).

Study and Analysis of Copy-Move Forgery Detection in Digital Image: A Review

Rachana[1], Ashok Kumar[2], H.L.Mandoria[3], Binay Pandey[4]

[1]M.Tech Student, Dept. of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India
[2, 4] Assistant Professor, Department of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India
[3] Professor and Head of Information Technology
G. B. Pant University of Agriculture & Technology, Pantnagar, India

---

Abstract - *In today's digital age, Digital image forgery becomes a common information falsification trend. This is generally done due to the largely available contemporary editing software and superior digital cameras. Authenticity of images becomes a more imperative issue while transferring data from one place to another place. Trustworthiness of photograph has a significant role in many areas - forensic investigation, criminal investigation, surveillance system, intelligent system, medical imaging and Journalism. Digital Image forensics finds the authenticity of the images. Different techniques are used to create forgery in the digital image. More regular type of digital image forgery is copy move forgery in which a part of an image itself is one copied and pasted into another location of the same image to conceal or alter the meaning. Post processing operations like resizing, blurring, rotation, JPEG compression etc has been done which makes digital image forgery detection difficult and hence an efficient approach is needed to detect the forgery into digital images. Copy Move forgery detection technique is grouped into two methods: Block based and Key Point based. In this paper, we have presented the various block based copy move forgery detection techniques. Image forensics is a fast growing research field and promises a convincing improvement in forgery detection.*

***Key Words*: Digital image, Digital Image Forgery, Copy-move forgery, Authenticity, Block-based methods.**

1. INTRODUCTION

Digital images in the current era play very important role in various fields. They are used in different applications in the area of military, news, medical diagnosis and media. Due to the development in technology of digital image, for example, cameras, software, and computers and the wide spread via the internet, digital image can be considered a premier source of information this time. With the enrichment of technology and availability of low-cost hardware and software editing tools, it is not crucial to change or forge the digital images without any visible traces [9]. Digital image forgery and manipulation of digital images in many cases is to intentionally affect the awareness of the recipient. In this situation Digital image forgery detection plays an important role in image forensics to provide authenticity of the image. There are many detection techniques are classified into two approaches [11] as shown in (figure 1): a) active; and b) passive techniques.

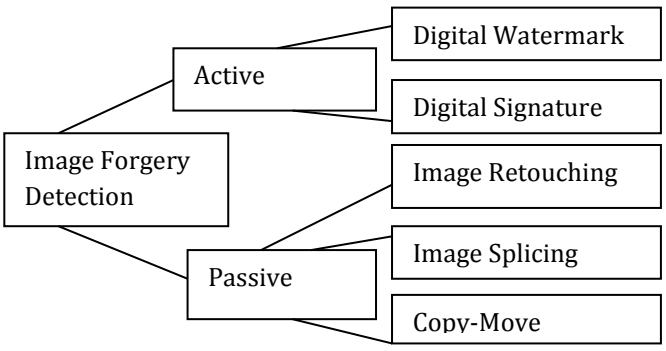


Figure 1: Image Forgery classification

For authenticity of a digital image, digital watermarking and digital signature have been proposed which are known as active techniques. In the active approach require some pre-processing operations, like attaching watermark and signature when producing digital images, thus limiting their applications in practice [14] not like the watermark and signature-based method, the passive techniques does not require any digital signature to be generated or to be inserted any watermark.

Passive authentication is the procedure of authenticating digital images without using any auxiliary information apart from the pictures themselves. Passive approaches

are further grouped into two categories: 1) source device identification; and 2) tamper detection. Source device identification: It is based on identifying camera fingerprints, which are the clues that are left by the image acquisition steps and the storage phases. Tamper detection: Tamper detection approaches are devised for particular types of forgeries, like copy-move or image splicing [26].

Image Retouching: It can be treated to be the less harmful/fatal kind of digital image forgery. Image retouching does not greatly transform or alter an image, but instead, enhances (or reduces) feature of an image. (Figure2)[10] Shows image retouching, and the difference between left image and right images (enhanced) clearly.

(a)Original Image (b) Image Retouching

Figure 2: Image Retouching

Image Splicing: This is another type of forgery. Image splicing is an approach that involves a composition of two or more images which are joined together to create a forgery as shown in (figure3) [17].This type of forgery is executed carefully; the border between the spliced regions can be hardly optically noticeable.

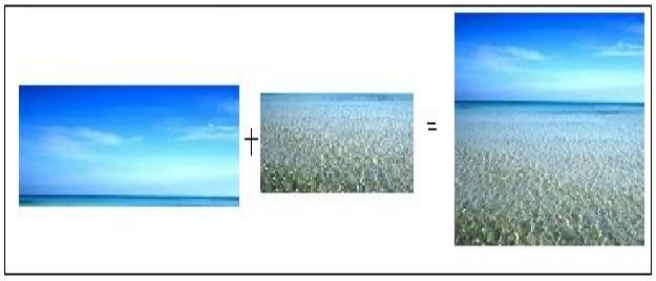


Figure 3: Image Splicing

Copy Move Forgery: Copy move forgery is more or less alike to image splicing. In this type of image forgery a part of an image itself is copied, moved to a desired location and pasted within the same image. (Figure 4) shows a red pen has been removed from the original image in part (a), by covering some of the region by background of the same image to produce forged image (b) [4]. There are many types of copy move forgery as follows: 1) just Copy-move;2) Copy-move with reflection; 3) Copy-move with different scaling; and 4) Copy-move with rotation[21].

(a) Original Image (b)Forged Image (Copy-Move)

Figure 4: Copy –Move Forgery

From the literature survey, copy move forgery detection techniques is further grouped into two methods as shown in (figure5): 1) Block based Method; and 2) Key point based Method

Block based Methods:

In Block based method divide the input image into overlapping or non-overlapping blocks of equal size. Then the feature is calculated for each block in order to detect duplicated regions. And matching is done to detect duplicated region in the image [21, 22].

Key Point-based Method:

Key point-based methods operate on whole image. Instead block based methods, Key point based methods compute their features only on image regions with high entropy. Key point based method can be further classified into two methods: SIFT (scale invariant feature transform) and 2) SURF (SpeededUp Robust Features) methods. [5, 3, 22]

2. GENERAL WORKFLOW OF COPY MOVE FORGERY DETECTION

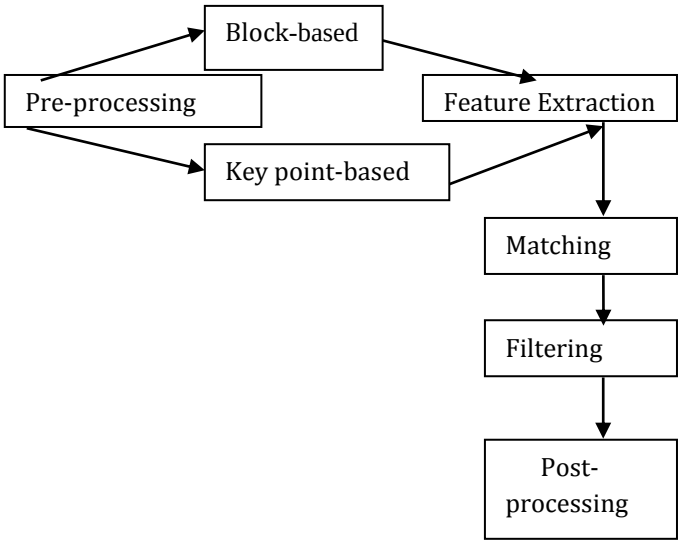


Figure 5: General Copy Move Forgery Detection

2.1 EXISTIN BLOCK BASED IMAGE FORGERY DETECTION TECHNIQUES

A large number of techniques have been proposed for detecting copy move forgery. A typical procedure has been followed as shown in figure 5.Copy Move Forgery Detection method can either block based and keypoint based approach. In block based approach, Most of the time in block based method needs gray scale images so the RGB image is first converted into a gray-scale image. For feature extraction, this gray scale image is divided into non overlapping/overlapping block of same size. From each block, a unique representation as a feature vector is computed. And then detect the copy move forgery by looking for the similar blocks [31].

Fridrich et. al [4] first analyzed the exhaustive search and then suggested a block matching method to espy copy move forgery. This method was based on Discrete Cosine transformation (DCT). Lexicographic Sorting is used and neighboring blocks are taken as possibly forged area. Thus these considered neighbor region are compared in the matching step .This technique in some complicated manipulation techniques like blurring or random noise addition it is not easy task to detect the forgery.

To make the computation faster, Popescu et. al [1] proposed a method based on Principal Component analysis (PCA).Due to the characteristics of PCA the number of features required to present a block were reduced as the half of the numbers of the features used by Fridrich. But this method is not robust to enough adequate small rotation of duplicated regions.

Li et. al [5] proposed a method based on (Discrete Wavelet transform) and Singular Value Decomposition (SVD). Discrete Wavelet Transformation (DWT) has been used to low frequency coefficients to reduce the feature vector representation and then SVD is applied on each sub blocks of low energy coefficient. This method works well even if the image is extremely compressed.

Myna et al. [2] proposed a method based on log-polar coordinate and Discrete Wavelet Transform (DWT). For the dimension reduction DWT is applied on the input image. And then sub blocks of the images are mapped on the log-polar coordinate to acquire a matrix corresponding to each block. Lexicography sorting is used to bring similar rows closer. Phase correlation was employed for similarity criterion. This method has lower time complexity. but not robust against geometric operation.

Q.Wu and S.Wang [26] attempted to make robust against post processing operation like scaling and rotation. Method was based on log-polar Fast Fourier Transformation (LPFFT).

Mohamadian and Pouyan [15] proposed a new method of detecting copy move forgery which is based on SIFT (scale invariant feature transform) algorithm along with the Zernike Moments. SIFT algorithm is used to perform detection but cannot detect flat copied region. To resolve this issue Zernike moments are used.

A method proposed by Bayram et al. [3] was based on Fourier-Mellin Transformation (FMT). By employing FMT on overlapping blocks of images, Features are extracted. These obtained features are robust to rotation and scaling, blurring, noise addition and JPEG compression. Lexicography sorting is used to neighboring the alike block and Counter bloom filter are used inspite of lexicography sorting to compare the blocks.

S.-jin Ryu and M.-jeong Lee [27] Zernike moments based detection approaches the flat copied region is detected and also invariant to different operations like JPEG compression, rotation, blurring and AWGN. The algorithm exhibited robustness against different degrees of rotation and high detection rate but not for the scaling.

Muhammad et al.[16] proposed a method based on Dyadic Wavelet Transform (DyWT) . Due to the characteristics of DyWT (shift invariant) is used. So, it is more applicable than discrete wavelet transform (DWT) for data analysis. In this method, decomposes the input image into approximation (LL1) and detail (HH1) subbands. Further those subbands(LL1 and HH1) are divided into overlapping blocks and after that measure the similarity between blocks. A method based on Dyadic Wavelet Transform (DyWT) in which both the LL and HH sub bands are used to find the similarity between the blocks of image.

Later on, same author Muhammad et al. [14] proposed a method to detect copy move forgery was based on undecimated wavelets and Zernike moments. UWT is translation invariant, although Zernike moments are scale and rotation invariant. Firstly undecimated wavelet transform is applied to find its approximation. After that Zernike Moments are calculated from the approximation. To find similarity of the moments between the blocks of image Euclidean distance is used. This algorithm is robust against different degree of rotation and high detection rate but not for the scaling.

A method to detect copy-move forgery using Discrete Wavelet Transform (DWT) and Principal Component Analysis-Eigenvalue Decomposition (PCA-EVD) is proposed by M. Zimba and S. Xingming [18]. DWT is applied on the image to reduce the size and obtained the low approximation coefficients. Principal component analysis to yield a reduced dimension representation .This technique accurately detects such specific image manipulations as long as the copied region is not rotated

or scaled. Later on, by the same author [19] a fast and robust approach is presented to detect copy move forgery. This method is based on block characteristics of DWT coefficients. Fixed window is then move over the sub-band, pixel-by-pixel, and a feature vector is obtained at each location. Thus these obtained Feature vectors, are sorted using radix sort. This method is robust to JPEG compression, noise addition and rotation through some fixed angles, the algorithm has good precision ration in detection of copy move forgery.

A method based on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) is proposed by Bashar et al. [20]. In this method input image is splited into small overlapping blocks. Each block of input imge is transformed by DWT or KPCA. DWT is applied on the image to minimize the size and obtained the low approximation coefficients. KPCA is used for feature collection and lexicographic sorting is used to cluster the alike feature blocks. This method is robust to manipulations such as translation-flip and translation-rotation of duplicate region

Yanping Huang et al. [34] An improved DCT-based method is developed to detect copy move forgery. Firstly, Discrete Cosine Transformation (DCT) is applied on fixed-size overlapping blocks of input image.DCT coefficient are obtained from each block to represent its features. To reduce the dimension of the features, Truncation is performed. Lexicography sorting is performed on calculated feature vectors. Duplicated region blocks are compared in the matching step. This improved DCT-based method is able to detect the duplicated regions even when suspected image was deformed by JPEG compression, blurring or additive white Gaussian noise.

Y. Cao and T. Gao [33] Firstly, Input image is divided into fixed-size blocks, and discrete cosine transform (DCT) is employed to each block, thus, the DCT coefficients is obtained for each block. Secondly, each cosine transformed block is presented by a circle block and four features are calculated to minimize the dimension. After that, Lexicography is used to sort the feature vectors, and duplicated region in the image is matched by predefined shift frequency threshold. The technique not only minimize the feature length but showed robustness against detection of multiple copy move forgeries, noise and blurring, but not robust to JPEG compression, rotation and scaling.

Sridevi, Mala and Sandeep [29] proposed a method for detection of copy move forgery in parallel environment. The methods begin with dividing the image into several blocks. Feature extraction is done for every block using intensity. The last two locations of the feature vectors store the block position. They established one more algorithm for parallel sorting. Lexicography sorting is done using radix sort method in a parallel way. They found the duplicated regions in the image by matching of features and these blocks are mapped on to the image using the location stored in the vector. This method shows improvement in performance over other conventional techniques.

Nguyen and Katzenbeisser [24] proposed a method which is based on radon transformation and phase correlation. In this method, Feature extraction is done by using Radon transform and phase correlation is used to match duplicated blocks. This proposed method is robust against rotation with angles smaller than 4◦ and Gaussian noise addition with SNR values larger than 35 db.

L. Li et al. [13] suggested a method in which image is first filtered and divided into overlapping circular blocks and then the features of the circular blocks are extracted by applying rotation invariant uniform local binary patterns (LBP). Feature vectors are obtained and then compared. And the forged regions can be located by tracking the corresponding blocks. This method is robust to JPEG compression, noise contamination and blurring, and also robust to rotation and flipping. The limitation of the proposed method is that when the region is rotated by common angles, it is difficult to detect the forgeries.

J. Zhao et al. [35] propose a method using Discrete Cosine Transformation and Singular Value Decomposition. In this method, 2D-DCT is employed to fixed-size overlapping blocks of input image. DCT coefficients are determined for each block. Further, each quantized block is divided into non overlapping sub-blocks and Singular Value Decomposition is used to each sub-block, then features are extracted to minimize the dimension using its greatest singular value. Finally, Lexicography is used to sort the feature vectors, and duplicated image blocks are matched by predefined shift frequency threshold.

Sunil Kumar et.al [28] suggests a method using PCA on DCT. Firstly DCT is practiced to calculate DCT coefficient for feature extraction and PCA to yield a reduced dimension representation respectively. Features, invariant to local change of intensity are created using down sampling of low frequency DCT coefficients. The method is robust against manipulation techniques like added noise and JPEG compression and also attend invariance to illumination, but it is fails in case of contrast variations. To overcome this limitation (contrast variations), same author [12] proposed a method based on binary DCT coefficients. In this method, input image is divided overlapping blocks and DCT is applied to blocks to calculate DCT coefficients. After that binary DCT features are extracted using sign of the DCT coefficients. Coefficient of correlation is used to match resulting binary vectors. This approach is robust against many manipulation techniques such as Gaussian noise addition, compression and minor rotation and scaling.

Table 1: Comparative study on Block Based Copy Move Forgery Detection techniques.

S. No.	Techniques	Method Used	Merits / Demerits
1	[4]	DCT	will not work in AWGN
2	[1]	PCA	robust against AWGN and JPEG compression
3	[5]	DWT-SVD	lower time complexity
4	[2]	DWT-log Polar coordinates	lower time complexity but the geometric operations are not discussed
5	[15]	SIFT	robust to geometric transformation
6	[3]	FMT	robust to scaling bussing, noise addition & SEEG compression
7	[6]	Zernike	high detection rate but not for the seating
8	[18]	PCA – EVD	will not work in rotation & scaling
9	[34]	Improved DCT	will not work in image distorted by JPEG compression ,blurring or AWGN
10	[28]	PCA on DCT	robust to against noise, IPEG compression and also achieve invariance to illumination

3. CONCLUSIONS

While going through the various papers on digital image forgery, which describes method for detection of copy move image forgery in digital image, it has been seen that a lot of work has been completed for copy move forgery detection. Thus further research effort is still needed to develop an appropriate algorithm that can detect the copy move. From the literature survey, we observed that the big problem with the copy move forgery in digital image is the detection of duplicated region processed by some common post processing operations such as compression, noise addition, rotation, scaling, flipping etc. The other concern is the time complexity of detection technique of copy move forgery in digital image. Motive of this paper was to give a brief comprehensive review about various techniques for copy-move forgery detection in digital images. A very common type of forgery i.e. copy move forgery detection is discussed. This paper presented a study on various detection techniques which is based on block method.

REFERENCES

[1] **A.C. Popescu and H. Farid** (2005) ***"Exposing digital forgeries by detecting traces of resampling".*** *IEEE Transactions on Signal Processing, vol. 53(2),* pp. 758–767.

[2] **A. Myna, M. Venkateshmurthy, and C. Patil**, 2007. ***"Detection of region duplication forgery in digital images using wavelets and log-polar mapping".*** in Conference on Computational Intelligence and Multimedia Applications. International Conference on, 2007, pp. 371-377.

[3] **Bayram, S., Sencar, H. T., & Memon, N.** (2009). ***"An efficient and robust method for detecting copy-move forgery".*** Paper presented at the Acoustics, Speech and Signal Processing. ICASSP 2009. IEEE International Conference on.

[4] **Fridrich, A. Jessica, B. David Soukal, and A. Jan** Lukáš. 2003. ***"Detection of copy-move forgery in digital images".*** in Proceedings of Digital Forensic Research Workshop. 2003.

[5] **G. Li, Q. Wu, D. Tu, and S. Sun**. 2007. ***"A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD".*** in Multimedia and Expo,IEEE International Conference on, 2007, pp. 1750-1753.

[6] **G. Muhammad and M. S. Hossain.** (2011). ***"Robust copy-move image forgery detection using undecimated wavelets and Zernike moments".*** in Proceedings of the Third International Conferenc on Internet Multimedia Computing and Service, 2011, pp. 95-98.

[7] **H. Farid** . 2009. ***"A Survey of Image Forgery Detection".*** Signal Processing Magazine, vol. 26, no. 2, pp. 16–25

[8] **Himanshu Sharma, Ashok Kumar and H.L.Mandoria**

"Study and Comparison Analysis of a Video Watermarking Scheme for different Attacks" International Journal for Research in Management and Technology, Volume-4, Issue-9, September-2015:pp. 51-56.

[9] **Harpreet Kaur, Jyoti Saxena.** 2015. **"Key-point based copy-move forgery detection and their hybrid methods: A Review**". Journal of The International Association of Advanced Technology and Science: ISSN-4265-0578.Vol.6

[10] **J. A. Redi, W. Taktak, and J.-L. Dugelay**.2011. ***"Digital image forensics: A booklet for beginners"*** .Multimedia Tool Appl., Vol. 51, no. 1, pp. 133_62.

[11] **Jiming Zheng and Liping Chang** .2014.***"Detection of Region-duplication Forgery in Image Based on Key Points' Binary Descriptors"***, Journal of Information & Computational Science, vol. 11, no. 11, pp. 3959-3966, Jul, 2014.

[12] **Kumar, Sunil, J. V. Desai, and Shaktidev Mukherjee** .2015. ***"Copy Move Forgery Detection in Contrast Variant Environment using Binary DCT Vectors".*** International Journal of Image, Graphics and Signal Processing (IJIGSP) 7.6 (2015): 38.

[13] **L. Li, S. Li and H. Zhu** .2013. ***"An Efficient Scheme for Detecting Copy-Move Forged Images by Local Binary Patterns"***, Journal of Information hiding and Multimedia Signal Processing, vol. 4, Jan., pp. 46-56.

[14] **M. Hussain,K. Khawaji,G. Bebis and G. Muhammad** . 2012. ***"Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform".***Digital Investigation, vol. 9, pp. 49-57.

[15] **Mohamadian, Z., & Pouyan, A. A.** (2013). ***"Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions***". Paper presented at the UKSim 15th International Conference on Computer Modeling and Simulation.

[16] **Muhammad G, Hussain M, Khawaji K, Bebis G**. (2011) "***Blind copy move image forgery detection using dyadic undecimated wavelet transform***". In: Proc. 17th digital signal processing (DSP) conference, Corfu, Greece; July.

[17] **M. P. Gomase and M. N. Wankhade** .2014. ***"Advanced Digital Image Forgery Detection: A Review***". International Conference on Advances in Engineering & Technology (ICAET), pp. 80-83.

[18] **M. Zimba, S. Xingming** .2011. ***"DWT-PCA (EVD) based copy-move image forgery detection".*** Int. J. Digital Content Technol. Appl. 5 (1) 251–258.

[19] **M. Zimba and S. Xingming**.2011.***"Fast and robust image cloning detection using block characteristics of DWT coefficients".*** JDCTA: International Journal of Digital Content Technology and its Applications, vol. 5, pp. 359-367.

[20] **M. Bashar, K. Noda, N. Ohnishi and K. Mori** . 2010. ***"Exploring duplicated regions in natural images".***IEEE Trans Image Process, (2010), pp. 1–40.

[21] **M. D. Ansaria, S. P. Ghreraa and V. Tyagi** .2014. ***"Pixel-Based Image Forgery Detection: A Review".*** IETE Journal of Education.

[22] **Mariam Saleem** *.2014.* ***"A Key-Point Based Robust Algorithm for Detecting Cloning Forgery". |*** *International Journal of Current Engineering and Technology, Vol.4, No.4.*

[23] **Mohd Dilshad Ansari** .2014. ***"Pixel-Based Image Forgery Detection: A Review".***IETE Journal of Education, vol 55, no.1

[24] **Nguyen HC, Katzenbeisser S.**(2012). ***"Detection of copy-move forgery in digital images using random transformation and phase correlation".*** Proceedings of the 2012 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP '12); July; IEEE; pp. 134–137.

[25] **P.Sabeena Burvin** *.2014.* ***"Analysis of Digital Image Splicing Detection".*** *IOSR Journal of Computer Engineering (IOSR-JCE) Vol. 16, Issue 2, PP 10-13*

[26] **Q. Wu, S. Wang, and X. Zhang.** 2011. ***"Log-polar based scheme for revealing duplicated regions in digital images".*** Signal Processing Letters, IEEE, vol. 18, pp. 559-562, 2011.

[27] **S.-J. Ryu, M.-J. Lee, and H.-K. Lee** . 2010. ***"Detection of copy-rotatemove forgery using zernike moments".*** in Information Hiding, pp. 51-65.

[28] **Sunil Kumar, Desai Jagan, and Mukherjee Shaktidev** .2014. **"DCT-PCA based method for copy-move forgery detection".** ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II. Springer International Publishing.

[29] **Sridevi, M., Mala, C., & Sandeep, S.** (2012). ***"Copy–move image forgery detection in a parallel Environment"***. Computer Science & Information Technology (CS & IT), 52, 19-29.

[30] **Sekhar Resmi and A S Chithra**.2014. ***"Recent Block based Methods of Copy-Move Forgery Detection in Digital Images"*** .International Journal of Computer Applications, vol. 89, no. 8, pp- 28-33.

[31] **Salam A.Thajeel, Ghazali Bin Sulong .**2013. ***"State of the art of copy-move forgery Detection Techniques: a review"*** .IJCSI Issues, Vol.10, Issue 6, No 2.

[32] **V. Tyagi** . 2010. ***"Detection of forgery in images stored in digital form".*** Project report submitted to DRDO, New Delhi

[33] **Y. Cao, T. Gao, L. Fan, and Q. Yang**. 2012. ***"A robust detection algorithm for copy-move forgery in digital images".*** Forensic science international, vol. 214, pp. 33-43.

[34] **Y. Huang, W. Lu, W. Sun, and D. Long** .2011 ***"Improved DCT-based detection of copy-move forgery in images".*** Forensic science international, vol. 206, pp. 178-184.

[35] **Zhao J, Guo J** .2013. ***"Passive forensics for copy-move image forgery using a method based on DCT and SVD"***. *Forensic Science International*; 233(1–3):158–166.

AUTHORS

Ms Rachana is pursuing her M.Tech. From the Govind Ballabh Pant University Agriculture & technology Pantnagar, Uttarakhand, India in Information Technology, She received her B.Tech. Degree in Computer Science & engineering from Uttaranchal Institute of Technology Dehradun, Affiliated to Uttarakhand Technical University Dehradun, India in 2012. Her interest includes Image Processing.

Mr. Ashok Kumar is currently working as an Assistant Professor in the Department of Information Technology College of Technology, GB Pant University of Agriculture & Technology. His area of interest includes Software Engineering, Software Testing & Software Analytics.

Dr. Hardwari Lal Mandoria is currently working as a Professor & Head in the Department of Information Technology, College of Technology GB Pant University of Agriculture & Technology, Pantnagar. His areas of Interest are Computer Networks, Network Security Wireless Communication, Mobile Computing, Information Security, Information communication Technology

Mr. Binay Kumar Pandey is currently working as an Assistant Professor in the Department of Information Technology College of Technology, GB Pant University of Agriculture & Technology. His areas of interest includes High Performance computing, Bio-informatics, Cloud-Computing.